الحرب الإلكترونية

الجزء الأول

الأمن السيبراني

تقديم مؤسسة كتائب الإيمان للإنتاج الإعلامي



١٤٤٥ - ٢٠٢٣

بسم الله الرحمن الرحمن

مؤسسة كتائب الإيمان

تقدم

سلسلة الحرب الإلكتروني

الجزء الأول: الأمن السيبراني

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

4/ 1445هـ - 11/ 2023 م

فهرس المحتويات

المقدمة

قال الله ﷻ (يَا أَيُّهَا الَّذِينَ آمَنُوا خُذُوا حِذْرَكُمْ)

قال أبو جعفر:

(يعني بقوله جل ثناؤه : "يا أيها الذين آمنوا"، صدَّقوا الله ورسوله ="خذوا حذركم"، خذوا جُنَّتكم وأسلحتكم التي تتقون بها من عدوكم لغزوهم وحربهم).

وعن أبي هريرة - رضى الله عنه - عن النبي - صلى الله عليه وسلم - أنه قال: «لا يُلدَغُ المؤمنُ من جُحْرٍ واحد مرتين».

(رواه البخاري ومسلم).

من منطلق إيماننا الراسخ بضرورة تطوير قدرات الإخوة في الحركات الجهادية من نواحي الأمن التقني فإننا نقدم الجزء الأول من سلسلة كتب الحرب الإلكترونية والمتعلق بالأمن السيبراني وسبل الحماية.

رغم وجود التطبيقات العملية في الكتاب إلا أن الشروح النظرية التي قد تبدو لك أخي القارئ مملة أحيانا سوف تعطيك نظرة عامة وشاملة على كل ما سوف تتعلمه لاحقا.

فهدفنا من هذا الكتاب ليس التلقين والتطبيق وإنما الفهم العميق لآليات عمل أنظمة الحماية، وإننا ندرك أنك سوف تعود لهذه الدروس النظرية دوماً كلما استشكل عليك أمر ما.

ولا ننصح أن تقرأه دفعة واحدة، بل تلذذ به وتعمق على دفعات، اقرأ السطر مرة ومرتين، افهم الكلمات ولا تحفظها، تخيل البيانات وهي تنتقل من هنا لهناك وما يحدث خلف كواليس التطبيقات والبرامج، ثم قم ببحثك الخاص وتوسع أكثر، فالقراءة مفتاح العلم، والعلم مفتاح النجاة والنصر بإذن الله تعالى.

خذ وقتك اللازم، اشرب فنجان قهوة، اقرأ فقرة واحدة كل بضع ساعات، لا تنتقل للتي تليها ما لم تفهمها جيداً.

لسنا ولست على عجلة من أمرنا، فأعطي الأمر الوقت الذي يستحقه.

في الكتاب فإننا لا نقوم بالتوصية ببرامج معينة للحماية ولا شرح طرق استخدام برنامج محدد من بينها، إنما نعلمك مفهوم الأمن السيبراني وآلية الوصول لأفضل حماية ممكنة مع طريقة اختيار البرامج والآليات التي تناسبك، ونترك لك حرية البحث واختيار الأفضل بالنسبة لك.

إخوانكم في القسم التقني – فريق الحرب الإلكترونية

مجلس التعاون الإعلامي الإسلامي

تعريف الحرب الإلكترونية

إن مصطلح الحرب الإلكتروني مصطلح كبير وباب واسع للغاية، وغالباً ما يأخذ الجانب العسكري والميداني (خارج عالم الإنترنت) منه النصيب الأكبر.

وما الحرب السيبرانية إلا جزء ونوع من أنواع الحروب الإلكترونية، وإننا بإذن الله تعالى سوف نستمر بإصدار سلسلة الكتب هذه حتى نغطي مجال واسع من أنواع وطرق هذه الحرب التي لم تعد حرب المستقبل فقط بل هي حرب الحاضر والواقع كذلك.

ومن الأمثلة على الحرب الإلكترونية هي أنظمة الرادار العسكرية، الطائرات دون طيار، محطات الإنذار والمراقبة، معدات الرصد والمراقبة.

بينما من أشهر الأمثلة على الحرب السيبرانية هي عمليات اختراق المواقع الإلكترونية أو الشبكات والتحكم بها.



الحروب السيبرانية – حروب الحاضر والمستقبل

وتنقسم الحرب السيبرانية إلى ثلاثة أنواع رئيسية وهي:

أولا: الهجوم الإلكتروني عبر الإنترنت

ثانيا: دعم الحرب الإلكترونية باستخدام الإنترنت

ثالثا: الحماية الإلكترونية عبر الإنترنت

وفي هذا الجزء من سلسلة كتب الحرب الإلكترونية هذه سوف نسلط الضوء على النوع الثالث من الحرب السيبرانية وهو الحماية عبر الإنترنت، كيف تحمي نفسك في العالم الرقمي؟.

بينما سوف نقدم في أجزاء تالية النوع الأول من الحرب السيبرانية والذي سوف يرشدك إلى تنظيم هجمات إلكترونية لغايات إيقاف أو عرقلة عدونا، تكبيده الخسائر وإحداث حالات من الفوضى في صفوفه، فضلا عن البحث حول السبل المتاحة لتطوير هذه الهجمات لتشمل قطاعات مختلفة وصولا إلى الغاية الأسمى وهو الهجوم في سبيل السيطرة والتحكم على الهدف.

ثم في جزء خاص سوف نقدم النوع الثاني من الحرب السيبرانية، حيث سوف تتعلم السبل والوسائل التي تمكنك دعم الميدان من خلال الحرب السيبرانية، مثل حرب الشائعات والحرب النفسية والإختراق وسرقة المعلومات وغيرها من الوسائل.

وبالطبع لا يمكن المضي قدماً في النوع الأول والثاني مالم تكن ذو خبرة وعلم في كيفية حماية نفسك، وإلا فعندها ستكون عمليتك الأولى هي الأخيرة وهذا ما لا نقبله، فنحن نحذر دوماً من ممارسة الحرب السيبرانية دون علم ودراية تامة بوسائل الأمن السيبراني وكيفية حماية نفسك.

وأود التنويه إلى أن الحرب السيبرانية بحد ذاتها هي عالم كامل يكاد لا ينتهي من التفاصيل والوسائل، إلا أنني أيه القارئ الكريم سوف أتدرج به حسب المستطاع، واسأل الله التيسير لنا جميعا يا رب العالمين.

الأمن السيبراني

قبل بداية الحديث عن الوسائل والطرق المتبعة لحماية اتصالاتك عبر الإنترنت، لابد من تعريف "الإنترنت" فما هو وكيف يعمل؟

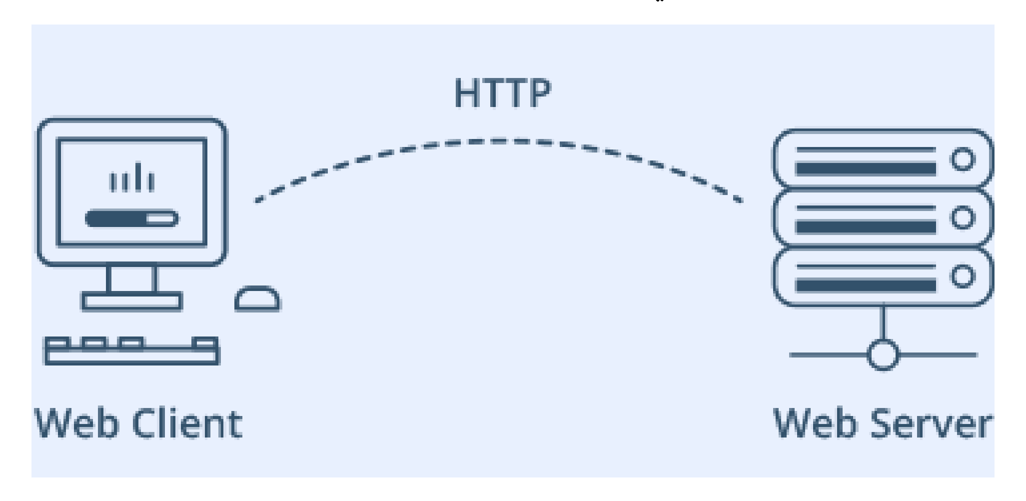
شبكة الإنترنت هي شبكة عالمية "لا مركزية". فلا يمكن بها الإجابة على سؤال مثل من يملك الإنترنت؟ في الحقيقة لا يوجد أحد حالياً يملك الإنترنت، هو بمثابة وقف عام لكل البشر.

تنتقل البيانات خلال هذه الشبكة بوسائل متعددة، للوصول إلى هدف واحد نهائي وغاية واحدة، الربط بين العميل والخادم ونقل البيانات بينهما باتجاهين.

العميل هو الشخص الذي يطلب البيانات، والخادم هو الجهة التي تقدم هذه البيانات.

على سبيل المثال: عند تصفح موقع جوجل فإن العميل في هذه الحالة هو أنت المتصفح، بينما الخادم هو شركة جوجل او سيرفرات شركة جوجل بصورة أكثر دقة.

وما بين العميل والخادم كلها وسائل وآليات مختلفة لبلوغ الهدف النهائي، وهو إجراء هذا الربط بين الطرفين، ونقل البيانات في كلا الاتجاهين.



العميل Web Client يقوم بطلب الخادم Web Server عبر بروتوكول التصفح HTTP

فمن الممكن أنك تتصفح شبكة الإنترنت من الهاتف الجوال، هنا يكون بينك وبين الخادم مجموعة من النقاط التي تنتقل خلالها البيانات وكذلك مجموعة من التطبيقات وأنظمة التشغيل، وهي التالية. (وقد يكون هناك المزيد فالأمر ليس ثابت دوماً)

- نظام التشغيل للهاتف -الأندرويد
- تطبيق متصفح الأنترنت -الكروم
- مزود خدمة الأنترنت -شبكة الهاتف
- مزود الأنترنت الرئيسي في البلد التي تتبع لها شركة الاتصالات

بينما في حالة تصفح الإنترنت عبر انترنت منزلي مثلاً، عندها عليك أن تضيف وسيلتين وهي الراوتر المنزلي، بالإضافة للسلك الموصل بينك وبين مزود الخدمة او البرج.

لذلك يمكن حصر انتقال هذه البيانات بطريقتين

- أولاً: سلكية
- ثانياً: لا سلكية

وقد يحدث ان تمر بياناتك عبر الحالتين، مثلا ان تنتقل بشكل لاسلكي من جوالك إلى مزود خدمة الإنترنت ثم يقوم هو بدوره بنقلها سلكياً عبر العالم.

الأمر لا ينتهي عند شركة الإنترنت ومزودها في البلد التي أنت بها، بل يتجاوز ذلك، لتوضيح الأمر دعنا نفترض أنك ترسل بريد إلكتروني من دولة عربية، يتم بدايةً تغليف البريد مع معلومات المرسل ومعلومات المستلم في حزمة واحده من قبل شركة البريد "الهوتميل"، الأمر يشبه تغليف شحنه لتوصيلها عند شركة توصيل البريد العادي.

ثم بعدها تنتقل هذه الحزمة من هاتفك او جهازك الكمبيوتر إلى الراوتر، ثم إلى أبراج الشركة، ثم إلى مزود خدمة الإنترنت الرئيسي في الدولة، والذي بدوره يرسلها عبر الأسلاك قاطعة دول مثل مصر، المغرب، عبر البحر إلى أوروبا ثم أمريكا. أو عبر البحر من تركيا إلى أوروبا ثم أمريكا، حسب الكيبل الرئيسي المغذي للإنترنت في المنطقة.

وهذا لأن شركة البريد الالكتروني -هوتميل- مقرها الرئيسي في أمريكا وسيرفراتها كذلك، فلا بد أن تصل حزمتك النهائي هناك.

هذه الآلية تنطبق على جميع أنواع التطبيقات، حتى تطبيقات المحادثة مثل التلجرام والواتس اب مع اختلاف دولة الشركة.

فمثلا إذا كانت الشركة للبريد الالكتروني روسية، فعندها سوف تمر حزمتك عبر نفس الطريق ولكن ستنتهي في سيرفرات الشركة الروسية بدلا من الأمريكية.

تخيل معي هذا المشهد في عقلك...

كتبت بريد إلكتروني عبر موقع او تطبيق "الهوتميل" أو "الجيميل"

قام الموقع أو التطبيق بتغليف الرسالة وعنوان المرسل وجميع بياناتك في طرد واحد ثم أرسله من هاتفك قاطعاً آلاف الأميال عبر العديد من نقاط توزيع الإنترنت وصولاً إلى جهته النهائية وهي خوادم أو سيرفرات شركة البريد الإلكتروني.

الخبر الصادم هو أن هناك عشرات الجهات في هذا العالم يمكنها التقاط هذا الطرد في اثناء رحلته هذه، والتي لا تستغرق أكثر من أجزاء من الثانية.

عشرات الجهات يمكنها التقاط حزمة بياناتك هذه في أثناء انتقالها من جهازك أنت العميل إلى الخادم!!

- ماذا يعني هذا؟ هل جميع حزم (طرود) بياناتي عرضة للسرقة؟

نعم، بالمعنى الحرفي هي عرضة للسرقة من كثير من الجهات.

- هل هذا يعني ان أمريكا يمكنها التجسس على حزم بيانات شركة روسية؟ أوالعكس؟

بالطبع يمكنها والسبب أنها ما زالت تستخدم شبكة إنترنت أمريكية ترتبط بقمر صناعي او كيبل إنترنت أمريكي.

- هل هذا يعني ان جميع اتصالات الروس ببعضهم تتجسس عليها أمريكا؟

لا بالطبع، لأن الروس وأي دولة في العالم وعلى نطاق حساس للغاية فهم لا يستخدمون قمر صناعي أمريكي ولا كيبلات أمريكية ولا شركات أمريكية، فتخرج الحزمة عبر إنترنت مملوك بالكامل لهم. وفي حالات أخرى فهم يقومون بتشفيرها بالطبع.

- أيهما أكثر أماناً، الإنترنت السلكي ام اللاسلكي؟

انتقال البيانات عبر وسط محمي وهو السلك الموصل بين العميل والخادم هو أكثر اماناً ، لأنه من السهل على الدول والجهات المختصة التجسس على بعضها البعض من خلال سرقة الحزم عبر انتقالها الفضائي بشكل لا سلكي.

الأمر يشبه إلى حد كبير جهاز "القبضة" اللاسلكية للتواصل بين الجنود، يمكن التجسس على اشارتها، والسبب هو انتقال هذه الإشارة عبر الهواء فيصبح لدى الجميع القدرة على الوصول إليها والتقاطها.

ولكن لا يمكن ابداً التجسس على مكالمة بين جنديين يتواصلان مع بعضهما عبر قبضة سلكية (جهاز الإرسال والإستقابل السلكي) حيث تنتقل بها الإشارة عبر وسط محمي بالكامل وهو السلك، لأنه في هذه الحالة يجب على الجهة الراغبة باختراق هذه المكالمة أن تضع شيء يقطع السلك نفسه لسرقة نسخة من البيانات أو إعادة توجيه الإشارة إلى جهة مختلفة.

- ماذا يحدث للحزمة التي خرجت من هاتفي بمجرد وصولها إلى سيرفرات الخادم؟

يتم فك الحزمة وقراءة بياناتها ومن ثم إعادة توجيه هذه البيانات إلى الشخص المتلقي.

وهو بدوره عند الدخول لبريده "في حال كانت الحزمة هي بريد إلكتروني" تنتقل حزمة مشابهة لها مرة أخرى من خوادم الشركة حتى تصل إلى جهازه.

- يبدو أن مهمة التجسس على الإنترنت سهلة للغاية!

ليس تماماً، على الرغم من أن معلوماتك وبيانات كلها عرضة للسرقة على طول الطريق بينك وبين الخادم! وعلى سبيل المثال لا الحصر فإنه من الممكن سرقة البيانات عبر إحدى أو جميع هذه النقاط

- الجوال نفسه إن كان مخترقاً
- تطبيق المتصفح الذي تستخدمه
- الراوتر إذا كان مزروع به برمجيات تجسس
- الأبراج ونقاط التوزيع إذا كان بها برمجيات تجسس
- مزود الإنترنت الرئيسي بالدولة
- جميع نقاط التقوية عبر سلك الإنترنت الرئيسي الذي يمر بالكثير من الدول حول العالم وصولاً إلى وجهة البيانات النهائية (وهذا الأخير يكون محمي بموجب اتفاقيات دولية)

نعم هذا صحيح فإنك معرض للسرقة في كثير من النقاط والأماكن، وليس فقط في الدولة التي أنت بها.

إلا أن الأمر ليس بالبساطة التي قد يبدو عليها...

فالخبر الجيد أن هذه الحزمة تنتقل بصورة مشفرة بالكامل، وهذا الأمر يعتمد على التطبيق الذي تستخدمه.

مثلا تطبيق التلجرام، عندما تكتب كلمة "مرحباً" وترسل إلى صديق.

يتم تغليف جميع بياناتك وتشفيرها بالكامل إلى حين وصولها إلى خوادم شركة التلجرام، وعليه حتى إن حاولت أي جهة على الطريق بينك وبين الخادم سرقة هذه الحزمة فهي لن تتمكن من معرفة ما يوجد داخلها ولن تستطيع فتحها.

وفي خوادم شركة التلجرام يتم فك الحزمة وإعادة توجيه الرسالة "مرحباً" إلى صديقك بعد تشفيرها من جديد.

- هل هذا يعني أن شركة التلجرام يمكنها التجسس على من تريد وقتما تريد؟

نعم بالضبط، وهنا يأتي دور مفهوم التشفير End to End

في هذا النظام من التشفير تضمن لك الشركة القائمة على التطبيق أن الحزمة لن يتم فك تشفيرها حتى في خوادم الشركة نفسها.

بل سوف يتم إعادة توجيه البيانات مباشرة إلى صديقك (المتلقي) وهي مشفرة بالكامل، حيث يتم فك التشفير في جهازه هو وتظهر له الرسالة "مرحباً".

وهذا هو أكثر وسائل التواصل اماناً -إن صدقت الشركة بالطبع ومثالنا هنا عن التلجرام-

- هل من الممكن أن تكذب شركات التطبيقات وتقول أنها تقدم خدمة تشفير كاملة وهي لا تفعل هذا؟

نعم قد تفعل وتكذب بخصوص هذه المزاعم، ولكن ليس في حالة تطبيقات ضخمة وعالمية مثل "الواتس اب" أو "التلجرام" فإن مئات ملايين البشر يستخدمونها، وهناك عشرات ومئات التطبيقات المنافسة التي تترصد غلطة واحدة لهم، وكذلك عشرات الجهات والفرق الإلكترونية الذين يعملون للتأكد من صدق الشركة فيما تدعيه.

ولهذا فإننا ننصح دوماً باستخدام التطبيقات العالمية المشهورة، اترك الأخرين يبحثون وفي حال وجود أي خلل أوشبهة في مزاعم التطبيق الأمنية عندها سوف نعلم ذلك من الآخرين.

- حسناً الوضع جيد جداً، إذا قمت بضامن أمن انتقال بياناتي عبر الإنترنت وتشفيرها فلا خطر بعدها..... صحيح؟

تقريباً هذا صحيح، لكن بالطبع كل ماتم ذكره أعلاه يكفل أمن البيانات بمجرد خروجها من جهازك حتى وصولها إلى جهاز المتلقي، بينما ما يحدث داخل جهازك فهذه مسؤوليتك أنت.

ففي حال كان الجهاز مخترق وتمكن شخص ما من سرقة بيانات الرسالة قبل تشفيرها من قبل البرنامج أوالتطبيق المستخدم فهو غير مسؤول عن هذا.

وهذه الحالات تحدث ونسميها الإختراق، أي تم اختراق الجهاز نفسه وعندها لن ينفع أي وسيلة تستخدمها لحماية بياناتك.

والسبب هو أن المخترق سوف يتجسس عليك أثناء كتابتك للبريد الإلكتروني، فعملية التشفير كلها في التطبيق تحدث بعد ضغطتك على زر الإرسال، وليس أثناء طباعتك للبريد، فالمخترق وبرمجياته الضارة سوف ترى جهازك بالضبط كما تراه أنت، وتسرق كل ما تفعله قبل أن يتم تشفيره.

وهنا فإننا ننصح مثلاً باستخدم برامج حماية الشاشة نفسها (سوف نتطرق لها بتفصيل أكثر لاحقاً) ، ولكن باختصار هذه التطبيقات سوف تمنعك من أخذ (سكرين شوت) أو صورة لقطة للشاشة وسوف تمنعك من تسجيل فيديو لشاشتك والكثير من الأمور الأخرى..

ماذا يعني هذا؟ هذا يعني أنه إن تمكن أحد من اختراق جوالك الشخصي فهو لن يرى إلا شاشة سوداء فقط، لأن هذه التطبيقات سوف تمنع التقاط أي صورة من الجهاز.

بالتأكيد ليست هذه وسيلة الحماية الكافية، حيث أن البرمجيات الضارة ليست بحاجة لرؤية شاشة جهازك كما تراه أنت، ولكنها واحدة من الوسائل وسوف نتطرق لها بالتفصيل لاحقاً.

من المقدمة أعلاه نصل إلى ضرورة تطبيق الآليات التالية للحماية...

أولاً: حماية الجهاز نفسه من الإختراق.

ثانياً: تأمين الجهاز في حالة تم اختراقه.

ثالثاً: استخدام تطبيقات تضمن التشفير End to End

رابعاً: إخفاء هويتك عبر الإنترنت بالكامل

لحماية الجهاز نستخدم تطبيقات برمجية خاصة مثل "مكافح الفيروسات"، "الجدار الناري" وتطبيقات حماية الشاشة نفسها.

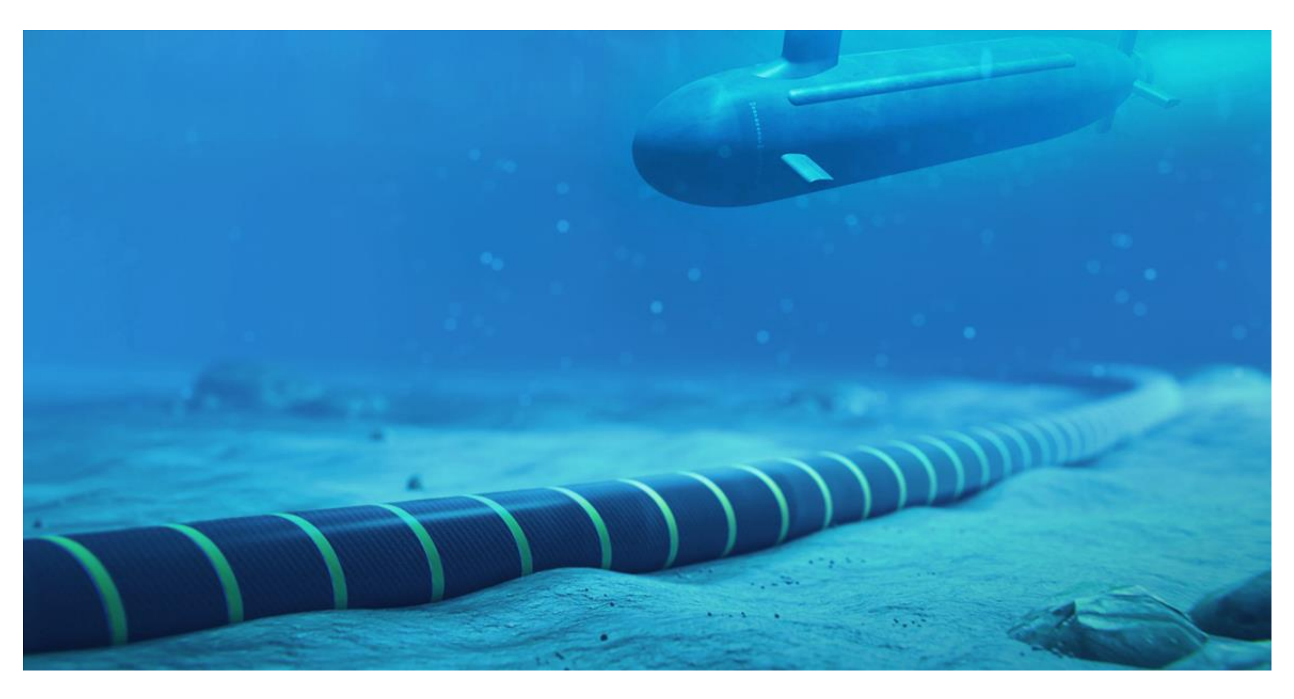
ولحماية الجهاز وتشفير الإتصال نستخدم الفي بي أن "Virtual private network VPN" والبرمجيات الخاصة بتشفير البيانات.

تنتهي مقدمة الأمن السيبراني وسوف نخوض في الفصول التالية بتفصيل أكثر حول وسائل الحماية المتبعة.

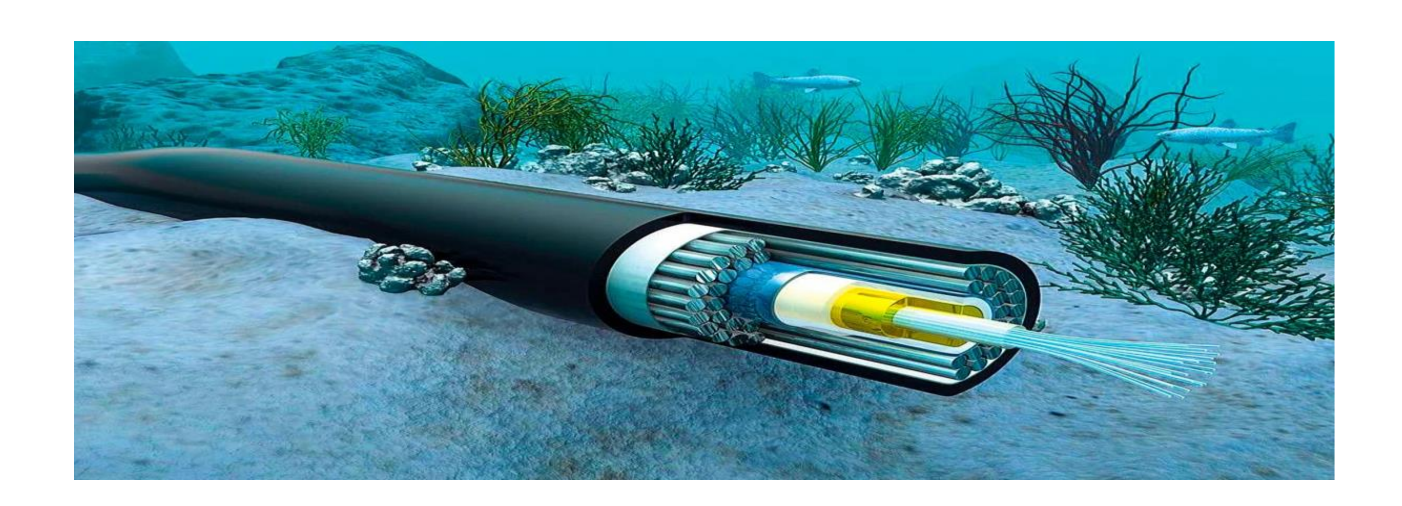
في نهاية هذا الفصل نود التنويه إلى أساسيات الأمنيات وهي عدم استخدام أي رقم حقيقي في التواصل أو في تفعيل حسابات مواقع الإنترنت وتطبيقات التواصل الاجتماعي.

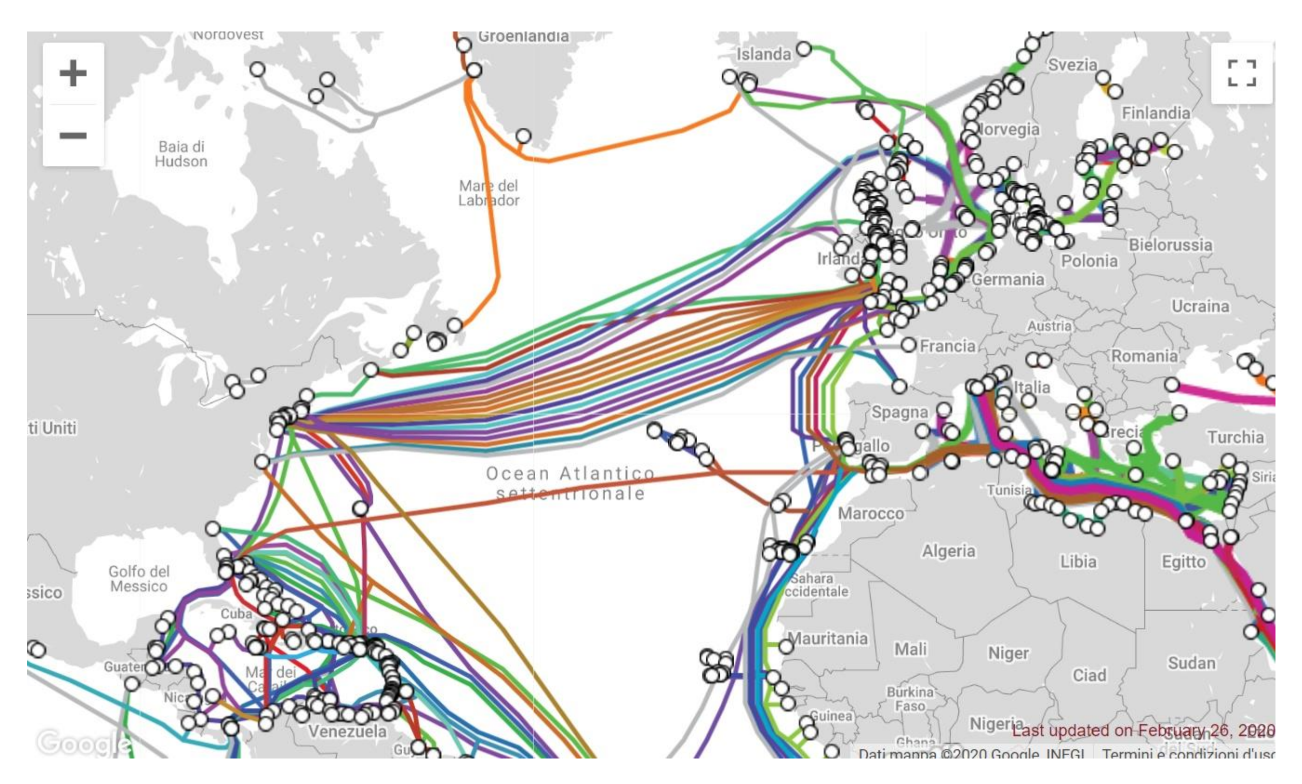
- من المهم دائما استخدام الأرقام الوهمية كما سوف يتم شرحه في الفصول التالية من هذا الكتاب.
- كذلك لا تستهين بخطورة كلمة المرور السهلة، اجعلها صعبة حسب التوصيات، حرف كبير وصغير ورقم ورمز.
- أيضاً لا تستخدم نفس كلمة المرور في أكثر من موقع، وهذا الخطأ يقع به الكثير من الإخوة للأسف، يستخدمون كلمة مرور واحدة في كل مكان.

لا تتردد بالتواصل معنا لتزويدنا بأفضل طرق الحماية التي إبتكرها أو استلهمتها من هذا الدرس وذلك عبر الطرق الرسمية المعتمدة.



تعتبر الكيبلات البحرية بمثابة العامود الفقري للإنترنت في العالم كله





يوجد حالياً أكثر من 430 كابلاً تحت الماء تعبر ما يقرب من 750.000 ميل (1.2 مليون كيلو متر) من قاع المحيط، يتبع الكثير منها لأمريكا حيث أنها تمتلك أكبر عدد من الكيبلات البحرية في العالم.

الفي بي أن (Virtual private network VPN)

- ما هو الفي بي أن؟ VPN

الشبكة الخاصة الإفتراضية (Virtual private network)، هي بروتوكول تشفير وحماية عبر الإنترنت، ببساطة وبدون تعقيد، الفي بي أن يعين نفسه وصي عليك وعلى هاتفك وعلى بياناتك، فلن يخرج كلمة من هاتفك ولن يدخل له كلمة، إلا عبر سيرفرات شركة الفي بي أن التي تستخدمها، والتي تكون منتشرة عبر العالم.

فعند استخدم تطبيق معين فإنه سوف يسطو على جهازك بالمعنى الحرفي، سيقوم بمنع دخول أي شيء وخروج أي شيء إلا من خلال المرور عبره أولاً، وعليه فهو سوف يحمي موقعك الجرافي "الآي بي IP Address" فكل البيانات تتم عبره وعبر الآي بي الخاص به.

فإذا كتبت "مرحباً" وأنت تستخدم الفي بي أن، فإن حزمة بياناتك لن تذهب إلى شركة "التلجرام" بل سوف تذهب إلى خوادم شركة الفي بي أن أولاً، ومن ثم هو من سوف يتولى إعادة توجيهها إلى التلجرام.

هذا يعني أن التلجرام نفسه لن يتمكن من معرفة عنوان الآي بي الحقيقي لك.

ليس فقط إخفاء الهوية، كذلك يعمل على تشفير إضافي لجميع الحزم الخاصة بك (ليس كل شركات الفي بي ان تقدم هذه الخدمة)، فإذا أرسلت رسالة على التلجرام، سوف يقوم بتشفير الحزمة المشفرة سلفاً من التلجرام، مما يعني ان شركة التلجرام نفسها لن يمكنها فك تشفير هذه الحزمة، حتى إن أرادت ذلك.

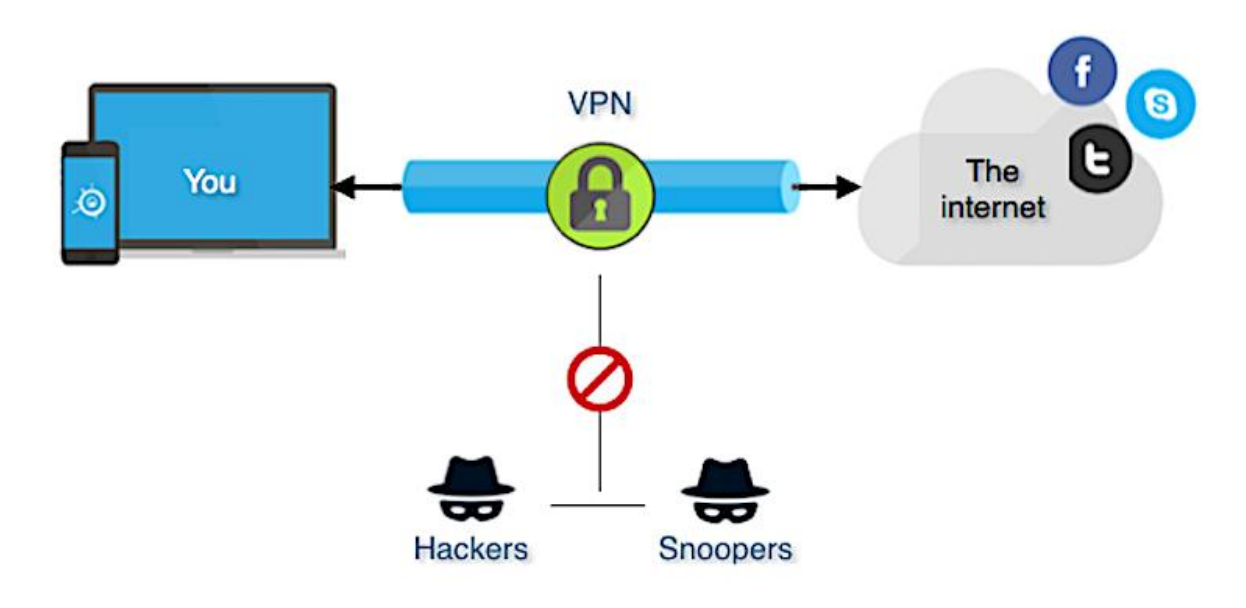
فالجهة الوحيدة المخول لها فك تشفير الحزمة هي شركة الفي بي أن.

وإذا شركة الفي بي أن فكت هذه الحزمة سوف تصطدم بتشفير التلجرام، والعكس.

وعليه إذا لم يكن هناك أي تنسيق بين شركة الفي بي أن والتلجرام على فك الحزمة فمن المستحيل أن تفكها جهة واحدة لوحدها.

فإذا قمت أنت بتركيب "في بي أن" صيني، واستخدمت تطبيق تراسل أمريكي، عندها لابد أن يكون هناك تفاهمات سرية بين الشركة الصينية والشركة الأمريكية ليتمكنوا من فك حزمتك. وذلك لأن كل جهة قامت بتشفير الرسالة بدورها، وعند فك التشفير سوف تصطدم بتشفير الشركة الأخرى.

وإذا قررت أن تعقد الأمور أكثر، وتدخل خادم روسي في الوسط بينهما، فعندها لابد أن يحدث تفاهم بين الثلاث جهات، ليتمكنوا من فك رسالتك المكتوب بها "مرحباً".



يقف ال VPN بينك وبين شبكة الإنترنت ويحمي خصوصيتك من المتطفلين ويقوم بتشفير بياناتك وإخفاء هويتك

الخلاصة المهمة هي التنوع

لابد بعد أن تكون قد فهمت آلية عمل الإنترنت والتجسس عليه، أن تحرص على أن تنتقل بياناتك عبر جهات متخاصمة وشركات يستحيل ان يكون بينها تفاهمات فيما يسمى "الحرب على الإرهاب".

- ولكن ماذا لو حدث تواصل وتفاهم بين الشركات؟ فالحرب على الإرهاب حرب عالمية وهذا موجود بالفعل والتنسيق قائم بين جميع دول الكفر العالمي!

حسناً في هذه الحالة عليك ان تقطع عليهم الطريق، من خلال استخدام في بي أن خاص.

وهذا موضوع ليس بالمعقد ولكن ليس بالسهل على أي أخ القيام به، لأنه يستلزم عمل سيرفرات وتركيب برمجيات تشفير داخلها، بحيث تنتقل الحزمة إلى الخادم الخاص بك وتشفيرها تشفير خاص بك، قبل أن ترسلها عبر العالم، والعكس.

ولكن هذا غير ضروري.

ورغم أنه قد يكون مطلوباً في مرحلة ما.... ولكن لا داعي لتعقيد الأمور على نفسك إلى هذا القدر، ما ذكرناه سابقاً كافي ووافي تماماً.

- كيف أختار أفضل تطبيقات الفي بي أن؟

قبل أي شيء أول ما عليك معرفته هو عدم إستخدام التطبيقات المجانية أبداً.

فكر للحظة، لماذا تقوم شركة بتصميم وبرمجة تطبيق يكلفها شهرياً مبالغ طائلة لتشغيله ثم تقدمه مجاناً لك؟ ماهو الثمن الذي سوف تدفعه بالمقابل؟

الثمن لن يكون بضع إعلانات يتوجب عليك مشاهدتها فقط، بل ستكون خصوصيتك هي الثمن الحقيقي الذي سوف تدفعه.

فالتطبيقات المجانية فضلاً عن انها تكون مصممة لغايات التشغيل فقط، ولا تقدم ميزات حماية أو شبكات إفتراضية قوية أو حتى تشفير حقيقي وجاد، فإنها تواجه تهم كبيرة بالتجسس على الخصوصية أو بيع المعلومات ومشاركتها مع جهات مختلفة.

وهذا لا يعني بالضرورة مشاركتها في ما تسمى الحرب على الإرهاب ...

بل إنها تبيع هذه المعلومات إلى شركات الدعاية الإعلانات مثلاً، ومراكز الدراسات والبحوث، وغيرها من الجهات العالمية الخاصة والعامة التي يهمها جمع البيانات، وبالطبع فالبيب من الإشارة يفهم، فمن يتاجر ببياناتك ويبيعها لشركات الدعاية والإعلان فإنه سوف يبيعها لكل من يدفع الثمن المناسب كذلك.

هل مازلت تذكر ما قلناه سابقاً عن استخدام التطبيقات والبرامج المشهورة عالمياً؟

نعم فهذه البرمجيات تكون تحت المجهر دوماً، عشرات المنافسين وفرق البحث والتقنيين يبحثون حول جدية ما تقدمة من حماية وأي شبهات لانتهاك الخصوصية.

لذلك فإن الأمر لن يكون مخفي عنهم إن فعلت شركة مثل هذا.

ولقد قمنا بالبحث حول توصيات المختصين لأغلب تطبيقات الفي بي أن المجانية كلها كانت توصي بعدم استخدامها لأسباب متعددة منها تهم بانتهاك الخصوصية ومنها ضعف في شبكاتها الإفتراضية وتسرب البيانات تقنياً ومنها عدم توفر تشفير قوي والعديد من الأسباب الأخرى.

بينما هناك الكثير من خيارات تطبيقات الفي بي أن الموصى بها عالمياً من قبل المختصين وللأسف فإن جميعها تطبيقات مدفوعة غير مجانية، الخبر الجيد هو ان أسعار الفي بي في متناول الجميع بمبلغ قد لا يتجاوز ال 5 دولار شهرياً.

التالي هي بعض أشهر انواع الفي بي أن المجانية، والغير موصى بها نهائياً

1- تطبيق SuperVPN

هذا واحد من أشهر التطبيقات، وهو تحديدا عليه توصيات سلبية بل تهم بالتجسس على المستخدمين

شاهد هذه الدراسة

https://www.safetydetectives.com/best-vpns/supervpn/#:~:text=Is%20SuperVPN%20safe%3F,visit%20and%20files%20you%20download

2- تطبيق Secure VPN

تقييمه 2 فهو مصنف غير آمن.

حسب هذا التحقيق والدراسة الأمنية التقنية التالية

/https://vpnoverview.com/vpn-reviews/secure-vpn

تقول الدراسة أن هذا التطبيق لا يحمي إتصالك بالإنترنت كما يتعهد، بل يتواجد به خلل تقني كبير يتسبب بتسرب معلومات الإتصال تقنياً، وهذا يعني أن عنوان الآي بي IP الخاص بك سوف يتسرب خلال إستخدامك لهذا التطبيق.

ورغم هذا فهناك خلل أكبر وغير تقني...

تقول الدراسة ان البرنامج أمريكي مسجل لشركة أمريكية رسمية وهذا يعني أن السلطات الأمريكية يمكنها سحب أي معلومات تريدها من خلال مذكرات الإستدعاء ، يعني من خلال المحكمة.

ولكن لحظة !!! إن الكثير من تطبيقات الفي بي أن أمريكية كذلك فهل هذا يعني ان بمقدورهم الحصول على أي معلومات يريدونها بمذكرة إستدعاء؟

بالطبع لا، وهنا يأتي دور التطبيق نفسه وميزة غاية في الأهمية، هل يقوم التطبيق أو برنامج الفي بي أن بحفظ البيانات من الأساس؟

كما ورد ذكره سابقاً فإن التطبيقات المجانية تقوم بهذا، والسبب هو أسباب تجارية فهذه البيانات، حركة مرورك عبر الإنترنت تعتبر مادة دسمة لتجارة الإعلانات والبحوث وغيرها، لذلك فهي تحتفظ بنسخة منها وهذا ما يفعله تحديداً هذا البرنامج.

وفي نفس الوقت التطبيق يطلب تسجيل دخول كامل، بريد إلكتروني ... الخ، وهذا فيه خطر مشاركة المعلومات مع السلطات الأمريكية.

3- تطبيق. Thunder VPN

للأسف يوجد عيب خطير في هذا التطبيق مشابه لما سبقه، وهو جمعه للبيانات

وعندما نقول جمعه لبيانات المستخدمين لا تعني بالضرورة أنه قدمها لجهات حكومية، ولكن اللبيب بالإشارة يفهم، من يجمع معلوماتك من أجل الأغراض التجارية فهو لن يتردد ببيعها كذلك لجهات حكومية.

الدراسة التالية تؤكد ذلك

https://www.top10vpn.com/reviews/thunder-vpn

هذه مشاكل التطبيقات المجانية، فعندما يقدم لك أحدهم شيء بالمجان عليك أن تعلم انك أنت السلعة.

عندما تقدم شركة تطبيق مجاني للفي بي ان ، لماذا؟

ماهي مكاسبها؟

بالطبع بياناتك وخصوصيتك واحده من أهم هذه المكاسب، حيث سوف تكون عرضة للبيع سواء لتجارة الإعلانات او لمراكز الدراسات او حتى لجهات حكومية.

- حسناً، سوف أبتعد تماماً عن التطبيقات المجانية، أخبرني كيف أختار التطبيق المدفوع وماهي هي معايير الإختيار التي علي اتباعها؟

أحد اهم الأمور التي تهم الباحثين في تحديد إن كان التطبيق آمن أم لا هو قيامة بحفظ سجلات للمستخدمين.

التطبيقات الآمنة لا تفعل هذا أبداً، فإذا دخلت موقع عبر الفي بي ان لن تحتفظ الشركة بأي نسخة بيانات من الآي بي الخاص بك أو البيانات المنقولة أو حركة مرورك عبر الإنترنت.

وطبعاً الأكثر أماناً هي تلك التطبيقات التي لا يتطلب التسجيل بها بريد إلكتروني ولا هاتف.

بالإضافة طبعاً لميزات التشفير التي يقدمها وباقي الخدمات التي سوف نذكر أهمها.

لاحظ ان موقع top10vpn يوصي بتطبيقات الفي بي أن في الرابط التالي كأفضل 10 تطبيقات، كلها مدفوعة وليس من بينها تطبيق مجاني واحد.

https://www.top10vpn.com/best-vpn/

وعلى سبيل المثال لا الحصر، سوف نقوم بشرح كيفية إختيار التطبيق الآمن بتجربة عملية على واحد من أشهر تطبيقات الفي بي أن العالمية وأكثرها تقييماً، برنامج البروتون Proton.

تطبيق بروتون تقييمه 8.8 من 10 وهذا تقييم ممتاز.

شاهد الدراسة الأمنية التالية

https://www.security.org/vpn/protonvpn/review/

الميزات التالية هي ميزات مطلوبة في أي برنامج في بي أن ويقدمها برنامج البروتون

1- لايقوم بتحزين أي بيانات نهائياً طوال فترة استخدامك له No Data Logging
2- لديه خيار "الكيل سويش Kill switch" وسوف يتم شرحه لاحقاً
3- تقسيم البيانات عبر الأنفاق وهذه ميزة أمان إضافية Split Tunneling
4- أي بي IP مشترك، وهذه ميزة أمان إضافية Shared IP address with other users
5- تشفير البيانات بالكامل أثناء إنتقالها من جهازك والعكس Network traffic encryption
6- سريع للغاية ولا يتسبب ببطىء في استخدام الإنترنت
7- يدعم شبكة التورينت Torrenting

التالي هي الملاحظات السلبية التي سُجلت على برنامج البروتون حسب الدراسة أعلاه

1- يتطلب تسجيل الدخول ببريد إلكتروني (للأسف أغلب البرامج تفعل ذلك وهي ميزة غير مرغوب بها)
2- السعر مرتفع للغاية مقارنة مع البرامج المنافسة
3- الدعم الفني بطيء

- ما هي خاصية الكيل سويش (Kill Switch) في برامج الفي بي أن، وكيف أقوم بتفعيلها؟

خاصية Kill Switch أو زر القتل توجد بتطبيقات الفي بي أن المميزة وهذا الخيار عند تفعيله فإنه سوف يعمل على قطع الإنترنت بشكل كامل من جهازك إلا من خلال الفي بي أن، فهو لن يجعل الإنترنت يعمل دون عمل الفي بي ان أولاً، فلا يوجد مجال للخطأ.

لكن في حالة عدم تشغيل ال Kill Switch

وعلى فرض أنه قد حدث خطأ في الفي بي أن عندها فقد تم فضح اتصالك لان الإنترنت سوف يستمر بالعمل بشكل طبيعي بدون الفي بي أن الى ان يعود للعمل ويحميك من جديد.

وخلال هذه الثواني التي يحدث بها هذا الخطأ سوف تكون مكشوف في العراء، بلا أي ميزات من الحماية التي يقدمها لك الفي بي أن ودون أن تعي أو تدرك هذا.

لذلك فإننا نوصي بشده أن تقوم بتفعل خيار Kill Switch داخل الفي بي أن، وهذا من إعدادات البرنامج

بالإضافة إلى ذلك فإننا نوصي بتفعيل الخيار التالي أو ما يشابهه دوماً

launch on start up التشغيل التلقاء عند تشغيل الجهاز

وهذا الخيار مع الكيل سويش سوف يعمل على قطع الإنترنت عن جهازك مباشرة عند الإنتقال من وضع الإطفاء إلى وضع التشغيل إلى حين إنتهاء الفي بي أن من التشغيل الكامل ثم السماح بمرور البيانات من خلاله فقط.

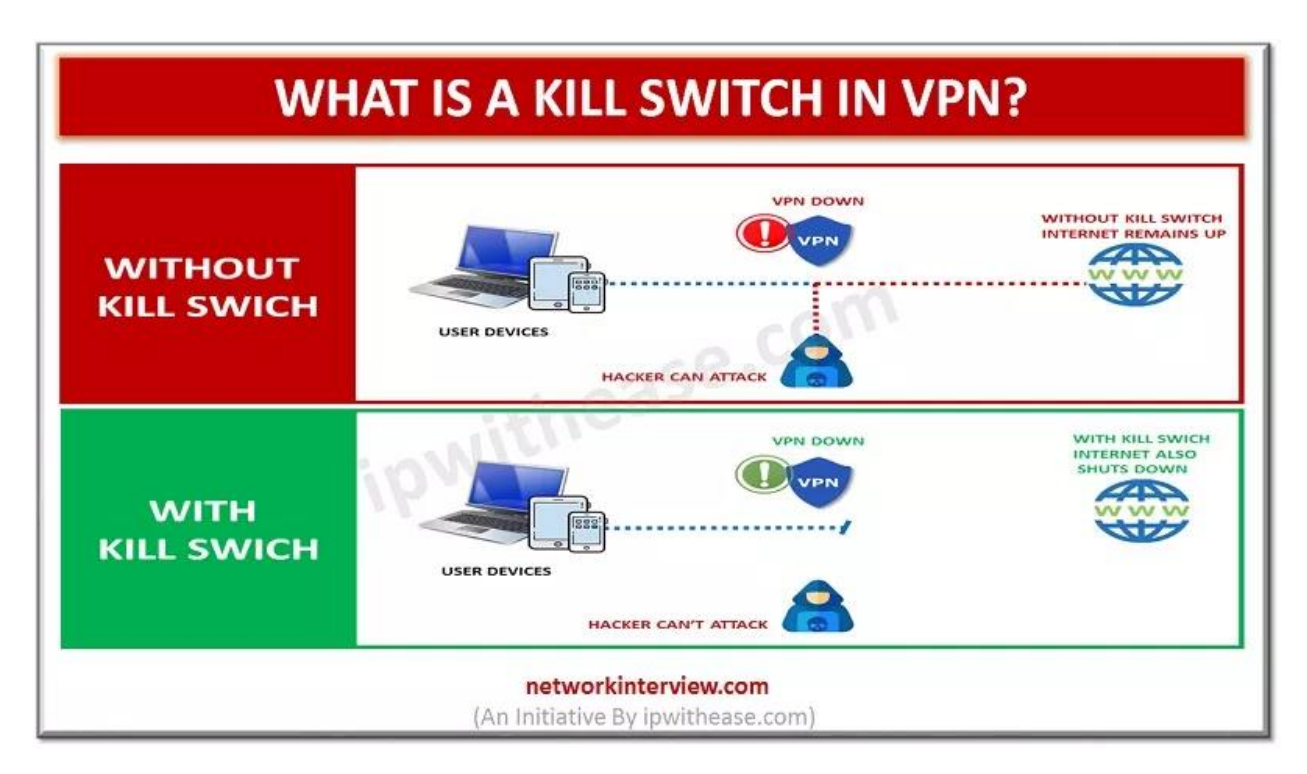
بينما في حالة عدم تفعيل هذه الخيارات فإن شبكة الإنترنت سوف تمر من وإلى جهازك قبل إنتهاء إقلاع الفي بي أن لثانية واحدة ربما، لكن هذه الثانية قد تكون الفارق بين الحياة والموت.

فالكثير من التطبيقات تعمل في خلفية الجهاز، مثل التلجرام والواتس أب، وقد تلتقط الأي بي الحقيقي الخاص بك خلال جزء من الثانية.

عندما يكون الفي بي أن في وضع التفعيل سوف يظهر في الهاتف على شكل مفتاح بجانب الساعة غالباً او بالطرف الأخر من الشريط العلوي.

للتأكد من انه يعمل ببساطة قم بفحص الأي بي الخاص بك عبر أي موقع لفحص الأي بي مثل هذا https://www.iplocation.net/

إن تم عرض أي بي IP يشير إلى دولة الفي بي أن التي اخترتها فهذا يعني انه يعمل، بينما إن ظهر أي بي يشير إلى بلدك الأصلي فعندها فإن التطبيق يواجه خلل في العمل.



في حالة تشغيل Kill Switch فسوف تبقى محمي حتى إن تم قطع خدمة ال VPN وذلك من خلال قطع إتصالك مع شبكة الأنترنت بالكامل

وهنا لا بد من الإشارة إلى ما يمكن تسميته بالنقطة الصفرية.

فماذا إن اشتريت هاتف لأول مرة، لابد حينها من الدخول للإنترنت لتحميل تطبيق الفي بي أن نفسه أول مرة، فإن دخلت على متجر جوجل فسوف يعرفون رقم الأي بي الخاص بك عن طريق البريد الإلكتروني الذي قمت بعمله لتتمكن من دخول متجر التطبيقات وبالتالي معرفة معلومات جهازك وبشكل خاص رقم IMEI الفريد الخاص بالهاتف الجوال.

حسناً سوف تقوم بعدها لا محالة بتركيب الفي بي أن، وعمل باقي إجراءات الحماية الخاصة والتي تعلمتها وسوف تتعلمها في هذه الدروس، وبعدها ستحذف البريد الإلكتروني وتغيره ثم تبدأ في إستخدام الجهاز في عملك الجهادي.

هل أنت في أمان تام عندها؟

كلا، فقد وقعت سلفاً في الخطأ الصفري وتركت خلفك كسرة خبز قد تدل عليك يوماً ما.

السبب هو أن رقم IMEI الفريد لجهازك مسجل حالياً في سيرفرات شركة جووجل ومرتبط به بريد الإلكتروني ذلك الذي توقفت عن استخدامه ولكن يرتبط به أيضاً عنوان الأي بي الخاص بك والحقيقي الذي قمت بإنشاء البريد من خلاله واستخدام متجر التطبيقات في تحميل الفي بي أن.

وبعد وقت طويل قد تنسى أنت هذا، ولكن جووجل لن تنسى، وفي حال سقط IMEI جهازك الخاص بيد أجهزة المخابرات بأي طريقة كانت، مثل أن تقوم بتحميل تطبيق غير موثوق أو تقع بخطأ تقني غير مقصود أو حتى من خلال التطبيقات الموثوقه إن كنت مطلوب دولياً على سبيل المثال، فعندها قد يتم الاستعانة بشركة جووجل للبحث عن IMEI جهازك وسوف يصلون إلى كسرة الخبز القديمة التي تركتها خلفك، وإلى الأي بي الذي استخدمته في ذلك الوقت.

ماهو الحل إذاً في هذه الحالة؟

جميع تطبيقات الفي بي ان لديها موقع الكتروني يمكنك تحميل نسخة التطبيق منها، لا تقوم ابداً بتحميل نسخة تطبيق من غير الموقع الرسمي للشركة فقط.

حيث تقوم بتحميلها على شكل ملف APK دون الحاجة لدخول متجر جوجل.

لذلك فإننا ننصحك قبل أن تبدأ إستخدام متجر التطبيقات أن تقوم اولاً بتحميل تطبيق في بي أن موثوق ثم تبدأ عمل باقي إجراءات الحماية.

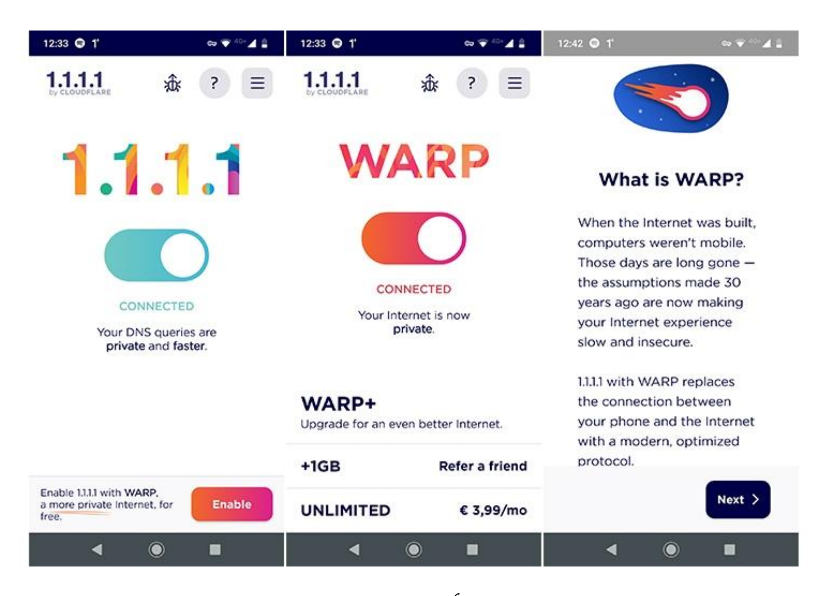
- هل يمكن تشغيل تطبيق في بي أن مع تطبيق تشفير إضافي أثناء العمل؟

نعم بالطبع، وهذا نوصي به بشده.

على سبيل المثال برنامج 1.1.1.1 أو ما يسمى Cloudflare WARP هو أحد خدمات شركة Cloudflare ذائعة الصيت في مجال التشفير والحماية عبر الإنترنت.

ورغم ما يشاع عنه أنه نوع من أنواع الفي بي أن، إلا ان هذا غير صحيح بتاتاً، فهذه الخدمة ليست بديلاً ابداً عن الفي بي أن، وإنما هي خدمة ثورية في مجال التشفير حيث سوف تنتقل جميع بيانات من جهازك وإلى جهازك مشفرة بالكامل عبر Cloudflare WARP.

إذاً لا يمكننا إعتباره بديلاً عن الـ VPN أبداً، ولكن هذه الخدمة هي خدمة ثورية في مجال التشفير والسرعة، فاذا كنت تريد المزيد من الحماية، استخدمه بالطبع مع في بي ان دون جدال، فسوف يقدم لك استخدام خدمة تشفير إضافية غير تشفير الفي بي أن طبقة حماية إضافية مختصة بالتشفير.

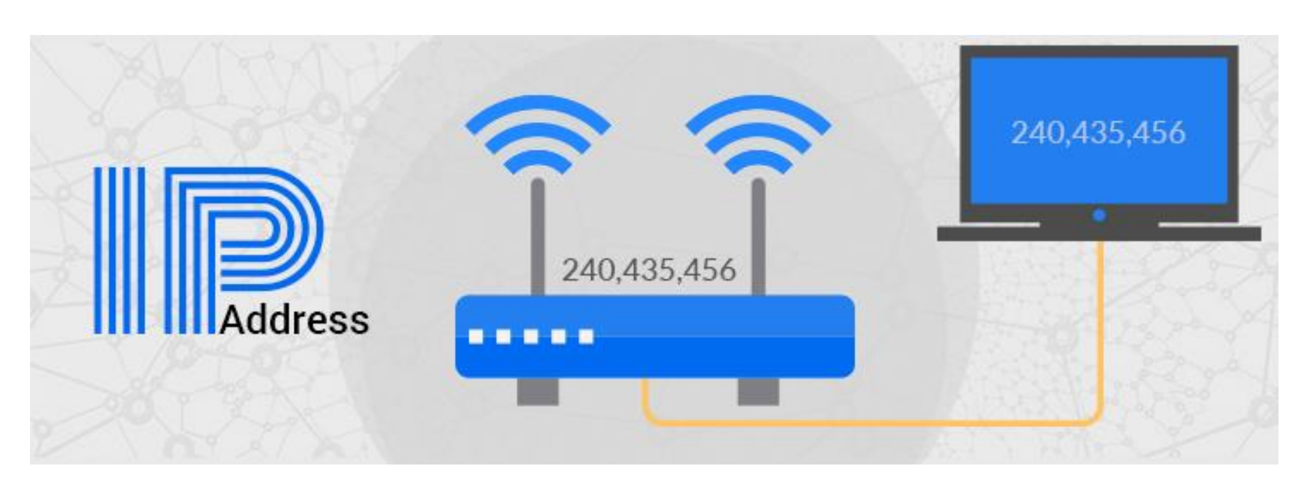


Cloudflare WARP تعمل على تأمين وتشفير جميع تواصلاتك عبر الإنترنت

بروتوكل عناوين الإنترنت IP address

- تحدثت كثيراً عن الأي بي (IP Address) فما هو وكيف يعمل؟

عنوان الأي بي IP Address ويعرف بالإنجليزية بـ Internet Protocol هو بروتوكول الإنترنت للعناوين، حيث تتعرف من خلاله شبكة الإنترنت على عناوين الأجهزة المرتبطة بها، ويمكنك إعتباره بالضبط كأنه عنوان منزلك التفصيلي بالشارع والرقم والبناية في حين أن الإنترنت هو صندوق بريد المراسلات اليدوية التقليدية، فليتمكن أحدهم من إرسال رسالة بريدية إليك فهو يحتاج إلى عنوان منزلك التفصيلي، وحسب نفس هذا المفهوم فإن عنوان الأي بي الخاص بك هو عنوانك التفصيلي الذي سوف يدل باقي أجهزة شبكة الإنترنت إلى جهازك.



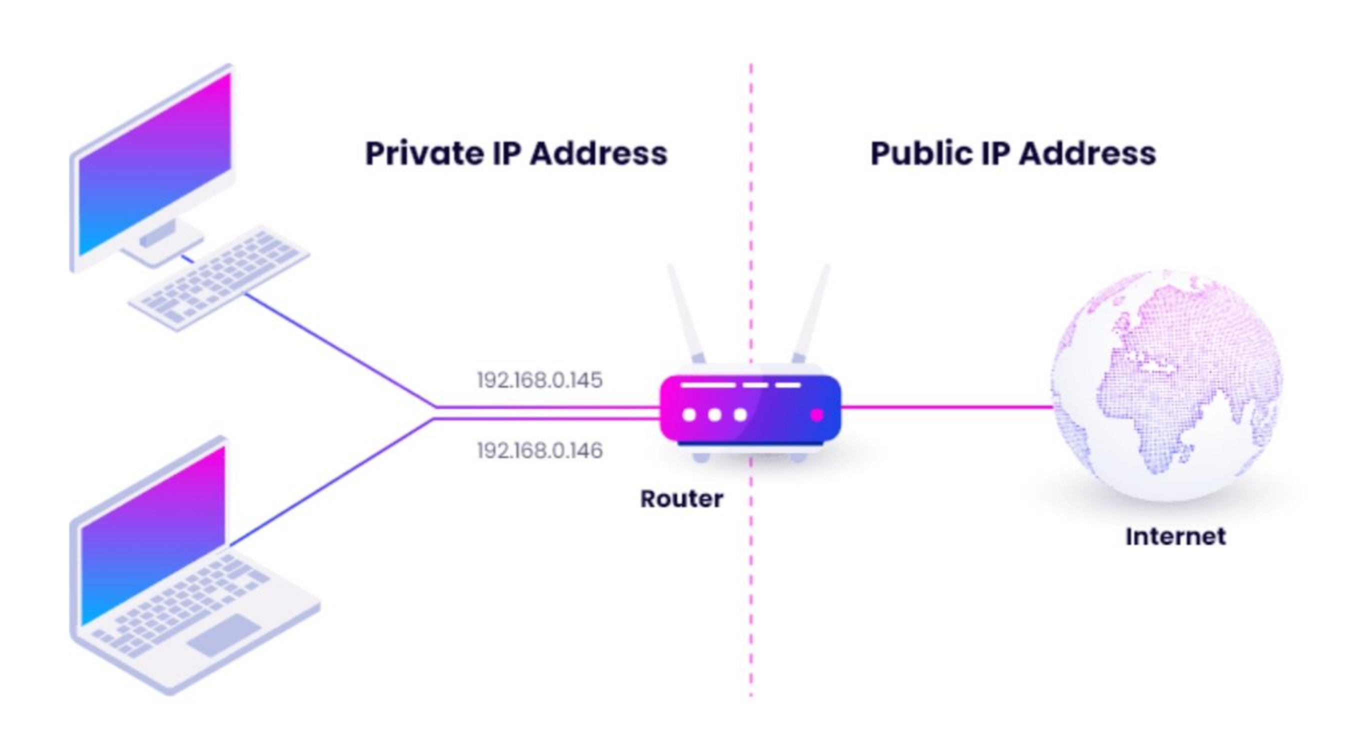
بروتوكل عناوين الإنترنت هو الطريقة التي تتعرف بها الأجهزة على بعضها البعض في الشبكة المعلوماتيه

وحسب المفهوم التقليدي فإن كل جهاز يرتبط بالإنترنت يمتلك أي بي خاص به باللحظة الزمنية نفسها، إلا ان هذا المفهوم غير دقيق تماماً.

فعلى سبيل المثال عندما يرتبط عدد من الأجهزة مع راوتر واحد فإن الأي بي لجميع الأجهزة سوف يكون هو نفسه وهو عنوان الأي بي الخاص بالراوتر، بينما سوف يقوم الراوتر بتمييز الأجهزة عن بعضها البعض من خلال أي بي داخلي أو محلي يسمى Local IP Address.

فعندما تقوم بالإرتباط مع الإنترنت عبر جهاز راوتر منزلي مثلا فإن عنوان ال IP العام الخاص بك سوف يكون هو عنوان ال IP لجميع الأجهزة الأخرى المرتبطة مع نفس الراوتر المنزلي، بينما سوف يقوم الراوتر بدوره بفرز هذه الأجهزة حسب أي بي محلي أو داخلي وهو الـ Local IP Address.

إذاً فبمجرد دخولك إلى الإنترنت فإنك تستخدم عنوانين للآي بي، العنوان العام الذي سوف يدل الشبكة على آخر نقطة توزيع إنترنت أنت مرتبط بها، ثم العنوان الخاص والذي سوف يدخل نقطة التوزيع هذه على جهازك بالتحديد من بين الكثير من الأجهزة الأخرى المرتبطة معها.



عنوان الآي بي العالمي (Public IP) يدل شبكة الإنترنت إلى الراوتر (Router)، بينما عنوان الآي بي المحلي (Private IP) يخبر الراوتر إلى أي جهاز عليه تسليم هذه البيانات ومن أي جهاز استلمها

- هل كل ما يحتاجه مخترق الأجهزة عبر الآي بي هو معرفة العنوان فقط؟

بالطبع لا، بالتأكيد سمعت عن خطورة عنوان الآي بي، وهو خطير بالفعل إن وقع بيد جهة ما يمكنها تحديد عنوانك التفصيلي واسمك ربما كذلك.

ولكن في حالات الإختراق فمعرفة عنوان الآي بي العام والخاص غير كافي ابداً.

فهذا العنوان معروف ويمكن للجميع معرفته بطرق عديدة كما أن كل موقع إلكتروني تدخله يمكنه معرفته كذلك مالم يمكن يستخدم تقنيات خاصة بحماية الزوار وإخفاء هوياتهم مثل التي تقدمها بعض الخدمات السحابية للمواقع الإلكترونية.

ومعرفة هذا العنوان لا تعني بالضرورة اختراق الجهاز، حيث أن المخترق يحتاج لأمر أخر غاية في الأهمية وهو المنفذ أو Port الذي سوف يخترق الجهاز من خلاله أو ما يطلع عليه مجازاً بالباب الخلفي.

وفي حين أن الآي بي العام و المحلي سوف يقود البيانات إلى جهازك مباشرة، إلا أن هذه المعلومات بمجرد وصولها داخل جهازك فهي ما زالت إلى الأرشاد! أين تذهب تحديداً؟

لنفرض أنك طلبت موقع جووجل عبر المتصفح، في هذه الحالة سوف يصل طلبك إلى شركة جووجل وبدورها سوف تعيد لك صفحة جووجل الرئيسية.

ولكن كيف سوف تعلم ان الذي طلبه هو فلان أي كيف سوف تستدل عليك؟ هذا يكون من خلال الآي بي االعام والمحلي ، فهي لن تعيد المطلوب لك تحديداً بل سوف ترسله إلى مزود الإنترنت الخاص بك ، وشركة الإتصالات سوف تستلم الطرد أو الحزمة وعليها عنوان المستلم، وهو الآي بي الخاص بك وسوف تسمح لها بالمرور إلى الراوتر الذي بدوره سوف يمررها إلى الجهاز عبر الآي بي المحلي.

ولكن بعد هذا أين سوف تذهب الحزمة في جهازك تحديداً

هنا يأتي دور المنفذ أو البورت Port.

البورت 80 على سبيل المثال هو بورت محجوز لبروتوكل التصفح HTTP

فعندما يرى الجهاز أن هذه الحزمة أو الطرد مطلوب تسليمها إلى بورت 80 فهو تلقائياً سوف يوجهها إلى المتصفح.

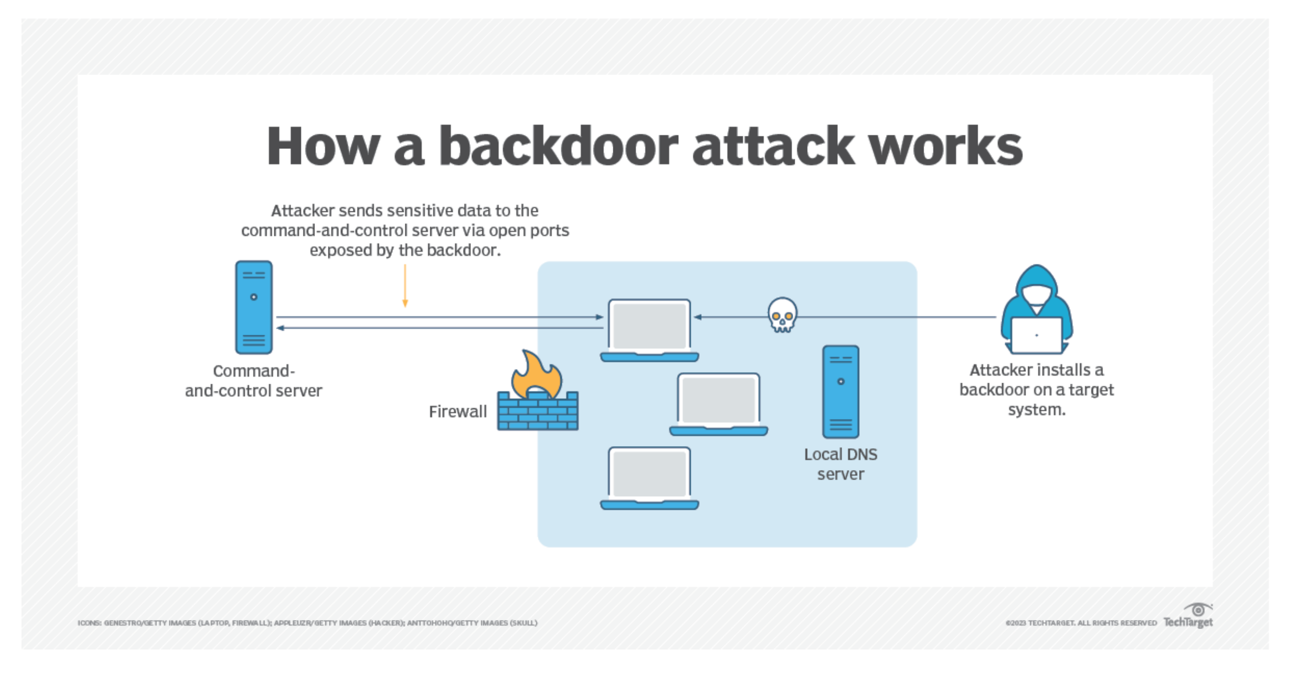
وعليه مثلا إذا تم إختراقك فإن المخترق سوف يفتح بورت خاص به مثلا 8022 وعبر هذا البورت سوف يتم ارسال البيانات إليه وكذلك استقبال أي أوامر منه، وهذا دون أن تعلم أو تشعر بذلك، وهذا ما نسميه بالباب الخلفي Back Door.

بعض البورتات تكون محجوزه سلفاً من نظام التشغيل مثل بورت 80 ولكن الجهاز يمكنه فتح ما يقارب 65000 بورت في اللحظة الواحدة.

وأقرب مثال على خطورة المنافذ هو المنفذ 3389 الشهير.

هذا المنفذ محجوز للإتصال البعيد مع الجهاز، ربما تعرف هذا الأمر عندما تقوم طوعاً بالسماح لشخص آخر أن يدخل جهاز كمبيوترك عن بعد ويستخدمه.

لذلك فإن أغلب أنواع الجدار الناري سوف تحظر هذا المنفذ تلقائياً لأنه خطير للغاية يمكن من خلاله دخول جهازك عن بعد، ولكن هذا لايعني ان برمجيات التجسس لا يمكنها فتح بورت أخر لنفس الغاية.



يقوم مخترق الأجهزة بتجاوز جميع أنظمة الحماية ويتواصل مع البرمجيات الخبيثة من خلال باب خلفي تقوم بفتحها له

وبالعودة إلى تطبيقات الفي بي أن وبرامج الحماية، فإن بعض أنواعها تسمح لك بإغلاق جميع المنافذ في الجهاز، ما عدا تلك الأساسية أو التي تستخدمها او تحددها انت، وعندها حتى إن كان هناك منفذ خلفي مجهول يستخدمة مخترق ما فإنه لن يعود قادر على إستخدامه.

فلن تتمكن هذه البرمجية من نقل او استقبال شيء ، وكأنك تسجنها داخل جهازك.

طبعا مالم تكن هذه البرمجيات تستخدم بورت أساسي في النظام، مثلا سمعت من قبل بالتأكيد عن الطابعات واختراق الأجهزة من خلال الطابعة ...

هذا لأن بعض برمجيات التجسس تستخدم بورت الطابعة الإفتراضي لنقل البيانات من خلالها.

تطبيقات الفي بي أن هذه سوف تحجب حتى بورت الطابعة مالم تكون تستخدمها وصرحت بفتح هذا البورت لوقت معين إلى حين انتهاء الطباعة.

إذا أردت حماية نفسك أكثر عليك دوماً تغيير البروتات الإفتراضية

مثلا البورت 3389 للاتصال عن بعد

ففي حالة كنت تستخدم هذا البورت وتحتاجه عندها الافضل تغييره الى رقم أخر مثلا 9911، ففي هذه الحالة لن يعلم المخترق ماهو بورت الاتصال عن بعد لديك.

ابحث عن طريقة تغيير البورتات في الجهاز.

ننصح باستخدام برامج الفي بي أن التي تقدم خدمات تغيير أرقام البورتات الإفتراضية والتي تسمح لك مراجعة وإغلاق جميع البورتات المشبوهة.

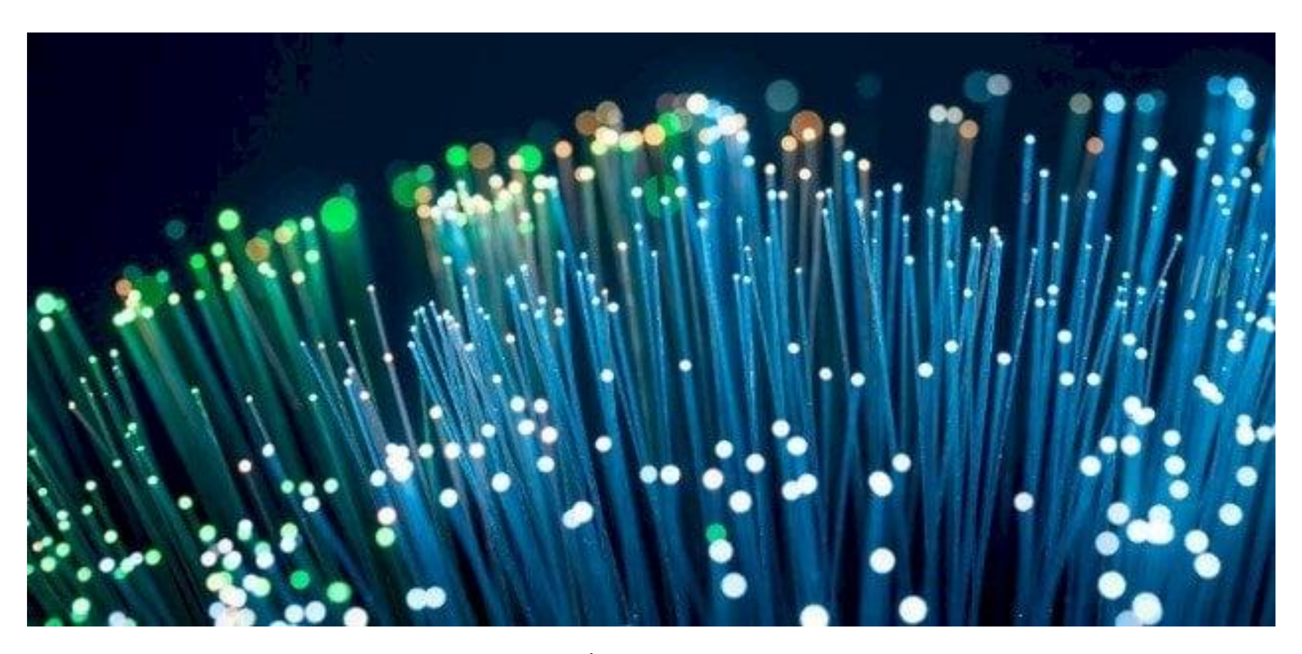
كواليس أبراج الإنترنت ومثال إدلب

في بداية هذه الدروس بينا أن الإتصال بشبكة الإنترنت يتم بواسطة طريقتين هما الإتصالات السلكية والإتصالات اللاسلكية.

بالطبع الإتصال السلكي أسرع كثيراً جدا من الإتصال اللاسلكي والسبب هو إنتقال البيانات بسرعات عالية عبر وسط محمي دون وجود أي مؤثرات جانبيه، هذه السرعة تساوي سرعة الضوء أي بسرعة الفوتونات . فكل إشارة سواء تلفاز أو انترنت أو راديو .. الخ هي في أصلها فوتونات وتتحرك بسرعة الفوتونات.

والفوتونات جسيمات غاية في الصغر تنتمي لعوالم ما دون الذرة، ولا تمكن رؤيتها ولا تتحقق رؤية شيء دونها، كونها المسؤولة عن نقل الضوء لشبكة العين التي تحوله إلى نبضات كهربائية.

قديما كانت الوظيفة الأساسية للفوتونات هي تحقيق عملية الإبصار من خلال نقل الضوء للعين، لكن هذه الجسيمات باتت تقوم بأدوار أساسية في كل مناحي الحياة، فقد مكنت العلماء من توظيف الأمواج الكهرومغناطيسية وأمواج البث الإذاعي والتلفزيوني، وصناعة أجهزة التحكم عن بعد وموجات الإتصالات التي تلتقطها الهواتف النقالة وأجهزة هبوط الطائرات وإقلاعها والشبكات اللاسلكية.



تنتقل الفوتونات عبر الألياف الضوئية أو البصرية بسرعة الضوء

حسناً بعيداً عن السرعة في نهاية الأمر سوف تنطلق هذه الفوتونات حاملة بياناتك عبر الأسلاك إلى وجهتها، إذا ضمنا بطريقة ما عدم وجود أي اختراق للسلك مثل تركيب أجهزة تجسس وسرقة البيانات عليه فنحن في أمان مطلق.

ولكن الأمر لا يحتاج اجهزة تجسس إن تم نقل هذه البيانات عبر الفضاء الكوني، او في الهواء مثلاً بما أننا نتحدث عن كوكب الأرض.

فهذه الفوتونات سوف تطير عبر الفضاء أي أن أي شخص يمكنه التجسس عليها، وذلك لأنه لايوجد عنوان ثابت تعرف أين تذهب له هذه الفوتونات.

مثلا في القبضة أو جهاز الإتصال اللاسلكي

عندما تتحدث به وتقول "مرحباً"

هذه الاشارة سوف تنطلق في الفضاء وكل جهاز إتصال لاسلكي متواجد في محيط قوة الإشارة أي في محيط مثلا 10 كيلو متر سوف يستطيع التقاط الإشارة وسماعها إن عرف درجة الموجة التي تم بثها عليه.

الموجة هي مثلا موجة الراديو إف إم، عدل الموجة وسوف تسمع إذاعة مختلفة عن الأولى وتكون هذه الموجة محجوزه لإذاعة معينة، وكل دولة تبيع هذه الموجات للإذاعات، ولهذا إذا كنت في منطقة حدودية ومعتاد على ان الموجة رقم 99 مخصصة لإذاعة القرآن الكريم فإنك قد تتفاجىء أن هذه الموجة لم تعد تلتقط إذاعة القرآن الكريم بل باتت تلتقط إذاعة للدولة الأخرى على الطرف الأخر من الحدود، هذا لأن تلك الدولة تكون قد باعات الموجة هذه على أرضها لإذاعة مختلفة، ولأن بث تلك الإذاعة أقوى من إذاعة القرآن فموجتها سوف تطغى ، وفي كثير من الأحيان سوف ترى صراع بين الإذاعتين، هذه تبث تارة ثم الأخرى وهكذا. يعني يحدث تداخل موجات.

بالعودة إلى أبراج الإنترنت...

بالتأكيد الإتصال السلكي هو الأكثر اماناً ولكن من هذا الذي يستطيع مد الأسلاك في كل مكان يصله الإنترنت؟ هذا الحل لن يكون عملياً بالتأكيد، لذلك فإن بث البيانات بطريقة لا سلكية هو الحل الأنجع والأسرع والأفضل، وهنا يأتي دور أبراج الإنترنت أو أبراج الإتصالات.

عندما ترسل بياناتك إلى برج هذا يعني انك أرسلتها بطريقة لاسلكية وهو سوف يعيد بثها بطريقة لا سلكية.

الحقيقة أبراج الإنترنت هي مجرد أبراج تقوية لا أكثر ولا أقل (بالمفهوم البسيط). وضيفتها التقاط الإشارة ثم إعادة بثها.



تعمل أبراج الإنترنت على إستقبال البيانات وإعادة بثها وصولاً إلى المزود الرئيسي

فإن كانت الإشارة الخارجه من جهازك تصل إلى 10 كيلو متر كحد اقصى فهذا يعني أنك بحاجة إلى برج بعد 10 كيلو يقوم بتقوية البث وايصال هذه الإشارة إلى برج أخر يبعد 100 كيلو متر وهكذا حتى تصل الإشارة إلى مركز الإنترنت الرئيسي في الدولة الذي قد يبعد عنك 2000 كيلو متر.

ولكن هذا كله بسرعة الضوء، أي سرعة الفوتونات، والتي يمكنها قطع 300 ألف كيلو متر في الثانية الواحدة.

بدوره فإن مزود الإنترنت الرئيسي في الدولة سوف يقوم ببث هذه الإشارات إلى العالم ولكن على الأغلب ليس بطريقة لا سلكية بل عبر كيبلات الإنترنت، أي الأسلاك التي تربط مزودات الإنترنت في دول العالم بعضها ببعض.



مزود الإنترنت الرئيسي يخضع لحراسة أمنية مشددة وإجراءات صارمة حيث أنه الباب الوحيد الذي يوصل الإنترنت في دولة ما مع بقية العالم، ويرتبط مع بقية العالم من خلال الكيبلات.

- ولكن من ماذا يتكون برج الإتصال نفسه؟

برج الإتصال هو مثل الراوتر بالضبط (بالمفهوم البسيط)، ولكن راوتر عظيم جداً يمكنه استقبال ترليونات البيانات وإعادة بثها.

لذلك كما يمكن اختراق الراوتر المنزلي بالتالي يمكن اختراق البرج، بل ويمكن زراعة أنظمة تجسس عليه.

وهنا سوف تطرح مثال مدينة إدلب المحررة في سوريا حيث أنها أكثر مدينة يمكننا ايضاح خطورة الابراج الغير قانونية بها، فجميع خدمات الإنترنت في إدلب تمر عبر أبراج غير قانونية.

فهمنا الآن أن كل الإشارات اللاسلكية والسلكية يجب أن تنتهي في مكان واحد وهو مركز الإنترنت الرئيسي في الدولة، فلو كان لديك ألف برج في النهاية كلها ليست أكثر من عملاء لهذا المركز وضيفتها هي إيصال البيانات له، وهذا المركز هو من يبث إشارتك خارج الدولة لأنه هو من يملك القدرة والصلاحيات للوصول إلى كيبلات الإنترنت الرئيسية او إلى موجهات الأقمار الاصطناعية التي يمكن من خلال بث الإشارة خارج الدولة. يعني لديه مفاتيح الأبواب.

وحتى تمتلك هذه القدرات أنت بحاجة لتصاريح دولية وهذه التصاريح لا يتم منحها لكل من هب ودب، حيث يجب ان تكون دولة بحكومة معترف بها دولياً، متواجدة ومعترف بها في الجهات الدولية المختصة.

مثلا حتى تتمكن من الحصول على ايبيهات IPs خاصة بك لابد لك أن تكون معترف بك كدولة في ال ICANN

Internet Corporation for Assigned Names and Numbers (ICANN)

مؤسسة الإنترنت للأسماء والأرقام المخصصة

وهي من تقدم الأيبيهات واسماء النطاقات ... إلخ

إذا لم تكن مشترك بها فمن المستحيل أن تتمكن من الحصول على هذه الخدمة حتى إن كنت قد أسست حكومة ولديك منطقة خاضعة تحت سيطرتك مثل إدلب على سبيل المثال. في النهاية هذه الحكومة غير معترف بها فإن ذهبت لهم فسوف يطردوك من الباب.

لذلك في إدلب لايوجد أي خدمات محلية للإنترنت وللحصول عليها تم ابتكار وسائل اخرى عبر تركيا. وهي من خلال تركيب أبراج إتصالات خاصة على الحدود التركية تلتقط اشارة من الإنترنت التركي وتبثها عبر أبراج أخرى عبر مناطق المحرر.

فإذا دخلت الإنترنت من إدلب فأنت بالنسبة للعالم غير موجود في إدلب بل موجود في تركيا، فآخر برج معترف به دولياً موجود في مدينة تركية حدودية مثلا ومنه يتم بث البيانات واستقبالها عبر أبراج غير معترف بها لا تتبع لشركة اتصالات معترف بها في تركيا.

وهذا السبب أنك إذا فحصت عنون الآي بي الخاص بك فسوف يقول لك أنك موجود في مدينة أزمير التركية مثلا في حين انت جالس في مدينة إدلب !!

السبب أن آخر برج معترف به من شركة الإتصالات التركية موجود في أزمير التركية وباقي الأبراج التي تمر منها الإشارة كلها أبراج شخصية أو محلية، قد تتبع لشركات تركية تعمل بلا تصاريح من هيئة تنظيم الإتصالات التركية.

هذا يعني شيئين....

الأول: جميع هذه الأبراج التي تعمل بصورة غير قانونية فهي لا تخضع للرقابة الأمنية اللازمة من قبل الحكومة التركية مثلاً.

ففي حين تفرض هيئة الاتصالات التركية قوانين صارمة وتقوم بحماية هذه الأبراج بنفسها بالبرمجيات اللازمة ومنع وصول أي شخص إليها والعبث بها، فإن هذه الأبراج الغير معترف بها والتي تعمل بما يشبه سوق سوداء للأبراج غير خاضة لهذا ابداً، أي أن صاحب البرج أوالفني الذي عمل على تركيبه ويعمل على صيانته يمكنه بكل سهولة فعل كل ما يريده دون أي ضوابط او مراقبة.

فيمكنه زراعة برمجيات تجسس وأجهزة تجسس وكل ما يخطر على بالك.

تخيل أن شخص يجلس في مدينة إدلب إن دخل الإنترنت وفحص عنوان الآي بي الخاص به قد يأخذه إلى مدينة إسطنبول التركية !!

ماذا يعني هذا؟ فمن إسطنبول إلى إدلب تحتاج عشرات الأبراج لنقل الإشارة وكلها أبراج غير نظامية وغير معترف بها في هيئة الاتصالات التركية !!

في بعض الأحيان قد يشير الآي بي إلى مدينة أنطاكيا مثلاً، هنا فآخر برج نظامي معترف به موجود على الحدود في مدينة أنطاكيا، هذه الشبكة أكثر اماناً من الشبكة التي بدأت بأبراج غير نظامية من اسطنبول بالطبع.

حسناً ماذا إن قال لك الأي بي أنك موجود في مدينة إدلب في سوريا !

- هل هذا يعني أن إدلب لديها إنترنت خاص بها ؟

لا هذا يعني أن معلوماتك كلها تذهب إلى النظام السوري...

لأن الجهة الوحيدة في هذا العالم المصرح لها فرز الأراضي السورية وتقديم أيبيهات لكل قرية او مدينة هو النظام السوري فقط، بما في ذلك إدلب وشمال حلب، لأنه دولياً فإن حكومة النظام السوري هي المعترف بها والمصرح لها تقديم الإنترنت لهذه المنطقة فقط.

لهذا فإن الأبراج القادمة من تركيا لا يمكنها تخصص أيبيهات خاصة بإدلب، فليس لديها التصاريح اللازمة، ولكن هذه التصاريح موجودة بطبيعة الحال عند النظام السوري فقط.

بالتالي إذا فحصت الآي بي الخاص بك وقال لك أنك في مدينة إدلب – سوريا فهذا يعني أن بياناتك تنتقل عبر الأبراج لتنتهي كلها في دمشق.

وهذا موجود فعلاً في إدلب حيث هناك شركات إتصالات تأخذ الإنترنت كله من النظام السوري، أي كمن تقدم بيانات الأنترنت في المناطق المحررة كلها هدية للنظام السوري على طبق من ذهب .

أي شركة إتصالات ، عراقية، هندية، ماليزية، فنزويليه، أختر أي دولة للشركة تحب إن أعطتك آي بي سوري فهذا يعني أن بياناتك سوف تنتهي في النهاية في دمشق.

إن اعطتك آي بي تركي يعني انها سوف تنتهي في تركيا وهكذا.

ولكن قبل أن تنتهي في دمشق وتركيا، فإنها قد تتعرض للسرقة والقرصنة عبر الأبراج الغير نظامية ، فهذه الأبراج لا تخضع للرقابة ولا لقوانين هيئة الإتصالات، بالتالي يمكن للفني العامل على البرج أو الجهة المشغلة له زراعة كل أنوع برمجيات وأجهزة التجسس فيه.

من الجيد أن تعلم ان الدول تحترم قوانينها...

على سبيل المثال فإن دولة مثل تركيا من المستحيل ان تسمح بان يتعرض برج نظامي يتبع لها للقرصنة، هي في النهاية سوف تجمع كل هذه المعلومات في مركز الإنترنت الرئيسي بطبيعة الحال أي انها سوف تذهب لها بكل الأحوال.

ولكن هذه الأبراج الغير نظامية ؟!! حدث ولا حرج

هذا قد يفسر لك سبب وجود أبراج غير نظامية بين اسطنبول وإدلب!!!

لان عمليات القرصنة على الإنترنت في المحرر هي عمليات كلها تتم خارج اطار القانون.

ولكن بالطبع ليس بعيداً عن نظر أجهزة المخابرات في تلك الدول.

وعليه فإننا ننصح أهلنا في مدينة إدلب بتوخي الحيطة والحذر من أي شبكة تنقل بياناتهم إلى دمشق المحتلة من النظام السوري النصيري، فجميع هذه الأبراج لم توجد إلا لتقديم بياناتكم هدية لهذا النظام.

كيف يمكنك معرفة هذا؟

ابحث في جووجل عن عنوان الأي بي الخاص بك مثلا الموقع التالي

https://www.iplocation.net/

وتأكد من دولتك

هام: بما يخص إدلب تحديداً وبعد سؤال عدد كبير من الإخوة فقد بدأ مؤخراً يظهر شبكة إنترنت إسرائيلية تستخدم بعض أنواع التخفي في الأبراج لتبدو أنها شبكة تركية، إلا أنه يمكن كشفها في بعض الأحيان، كانت التأكيدات مكررة أن هناك شبكة إنترنت إسرائيلية تم إدخالها إلى إدلب برعاية رسمية.





لقطة شاشة حقيقة لتطبيق التلجرام لجهاز متصل من إحدى شبكات الإنترنت من داخل إدلب مدعومة بشكل رسمي من الجهات المختصة في المدينة.

لايمكن كشفها بسهولة إلا أن غطاء الحماية ينكشف عنها في بعض الأحيان

حالياً يمكن كشف هذه الشبكة الإسرائيلية ببعض الطرق يمكن للجميع فعلها.

- إذهب إلى تطبيق التلجرام ثم إعدادت الخصوصية ثم عرض الجلسات، أنظر إلى أسم الدولة أسفل جلستك (قد تظهر إسرائيل في حال كنت تستخدم شبكة إسرائيلية دون أن تعلم)
- لن تتمكن من دخول عناوين كشف الأي بي كلها عبر الإنترنت لفحص الأي بي الخاص بك (أكتب في جووجل My Ip Address) وحاول دخول مواقع كشف الأي بي الخاصة بك، أشهرها وأفضلها محجوب ولن تسمح لك الشبكة بالولج إليه.
- ابحث في جوجل عن (VPN Detection أو Proxy Detection) مثلا هذا الموقع ipinfo.io شاهد تحليل معلومات الأي بي الخاص بك إن ظهر بها أن vpn أو proxy فعال في شبكتك وأنت لا تستخدمه فعندها قد يكون هذا مؤشر على وجود غطاء مزيف من قبل الشبكة لإخفاء دولتها الحقيقية أو برمجيات خاصة لإعادة توجيه البيانات.
- بعض المواقع التي تتعرف على الآي بي سوف تتعرف عليك تلقائياً أنك في إسرائيل، استمر بالبحث عن مواقع كشف الآي بي العام الخاص بك وجرب أكثر من موقع حتى تتأكد أن الشبكة غير إسرائيلية.

- كيف ولماذا تدخل شركات تتبع للنظام السوري وإسرائيل إلى مدينة إدلب وتسرق بيانات المستخدمين كلها؟

هذه الشركات تدخل كلها بتفاهمات وتصريح رسمي مع الجهات المعنية داخل البلد أو المدينة من خلال دفع مبالغ مالية طائلة تحت شعار ترخيص أو تصاريح عمل.

التبرير الوحيد لوجودها هو سرقة البيانات والتجسس ومراقبة المستخدمين.

- هل يمكنني الإرتباط بالإنترنت بدون الأبراج؟

نعم هذا نسميه الإنترنت الفضائي وهو أن تخرج الإشارات من هاتفك او راوترك مباشرة إلى القمر الصناعي، وعلى عكس ما يشاع أنه أكثر اماناً فهذا غير صحيح .

قد يكون أكثر اماناً في عملية نقل البيانات فقط، ولكن أنت تقدم نفسك كلك بجسدك هدية للقمر الصناعي لأنه سوف يكون قادر على تحديد مكانك بالسانتي متر الواحد.

فضلاً عن أن هذا النوع من الإتصالات لا يستخدم إلا من قبل محطات التلفزة والأخبار وعلى نطاق مختلف ضيق جداً، فكل من يستخدمه عليه علامات سؤال، من هو هذا؟!



في الإنترنت الفضائي فإن الراوتر يرتبط بشكل مباشر مع القمر الاصطناعي مجاوزاً كل نقاط التوزيع في العالم، وهو أكثر اماناً بالتأكيد ولكنه مثير للريبة حول هوية مستخدميه، كما يمكن تحديد موقع المستخدم بدقة متناهية.

الحماية من التتبع والمحاكيات وطبقات الحماية

إن تم إختراق جهازك، فلن تنفعك أغلب وسائل الحماية المتبعة.

وذلك لأن المخترق سوف يقوم بفتح باب خلفي (منفذ خلفي أو بورت خاص) داخل جهازك سوف يقوم بسرقة معلومات الجهاز وكل ماتفعله قبل أن يتم تشفيره من الأساس ويرسل نسخة منه إلى المخترق، كذلك سوف يستمر بمتابعة عناوين الآي بي الخاصة بك العامة والخاصة ويرسل تحديثات مستمرة لها، فأغلب وسائل الحماية لن تكون مفيدة في هذه الحالة. لذلك فإننا ننصح بحماية جهازك أولاً.

- كيف أحمي جهازي أولاً؟

ليس من السهل حماية جهازك الشخصي، بالتأكيد مطلوب منك تركيب برمجيات الحماية من الفيروسات، والجدار الناري لمنع الاختراق، تطبيقات الفي بي ان لإخفاء "الاي بي" وفحص البورتات أو المنافذ باستمرار مع إغلاق ومنع مرور البيانات من الغير مستخدم أو المشبوه منها.

ورغم هذا كله يمكن اختراق الجهاز، فالعدو متقدم تقنياً للغاية.

أول توصية نوصي بها هي عدم استخدام جهاز من الأصل، التوقف تماماً عن استخدام الهواتف النقالة، واستبدالها بأجهزة اللابتوب مع استخدام محاكيات الجوالات.

الأجهزة يجب ان تكون بمعالج قوي وبنفس الوقت صغيرة الحجم يمكن حملها بسهولة، والأهم هو مع عدم وجود كميرا داخلها وعدم وجود نظام المواقع الجغرافية "الجي بي أس".

هذه الأجهزة متوفرة بالسوق، يكفي ان تطلب جهاز بمواصفات محدده، بدون كميرا وبدون جي بي أس، ولعدم إثارة شكوك البائع اقرأ جيداً مواصفات الجهاز واحرص على أن لا يكون من بينها نظام التتبع الجغرافي ولا الكاميرا.

وفي حال تعذر الحصول على جهاز بدون كميرا، يمكن تغطيتها ببساطة بالطريقة التقليدية، بينما لا تقتني ابداً جهاز مدمج فيه نظام التتبع الجغرافي "الجي بي أس".

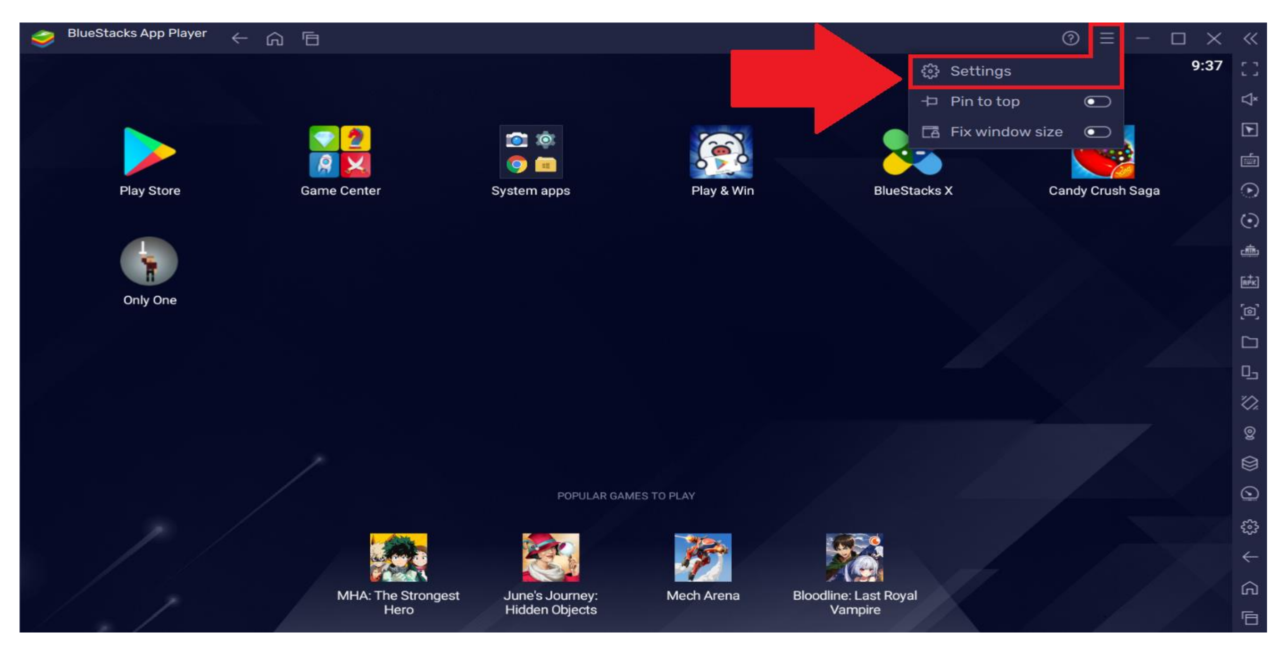
- كيف سوف استخدم تطبيقات الهاتف الجوال من خلال اللابتوب؟

لا تستخدمها مباشرة، فالتلجرام وجميع التطبيقات تقدم نسخة لنظام تشغيل ويندوز أو باقي أنظمة تشغيل اللابتوبات، ولكن لا تستخدمها.

عليك استخدام محاكيات الجوال...

وهي تطبيقات برمجية تقوم بتحميلها على اللابتوب، تسمح لك بعمل أجهزة خلوية وهمية في جهازك، بالعدد الذي تريده.

على سبيل المثال المحاكي التالي BlueStacks x
https://www.bluestacks.com
من أكثرها شهرة، ولكنك غير ملزم باستخدام هذا المحاكي تحديداً، يمكنك البحث عن بديل له.



يمكنك من خلال محاكيات الجوال عمل أي عدد تريده من الهواتف الوهمية داخل جهاز الكمبيوتر الخاص بك متجاوزاً كل المخاطر المترتبة على استخدام الهاتف التقليدي

بعد عمل الهواتف الوهمية في جهاز اللابتوب سوف تنتقل حماية اللابتوب إلى الهواتف الوهمية تلقائياً، أي أن كل مكافح فيروسات وبرنامج في بي أن تستخدمه فهو سوف يحمي اللابتوب بما فيه المحاكيات.

حيث بالطبع ستكون قد قمت بتركيب مكافح الفيروسات، الجدار الناري، الفي بي أن، حماية الشاشة.

وبشكل تلقائي سوف تعمل حماية اللابتوب على حماية الهواتف الوهمية.

ولكن كطبقات إضافية للحماية، يمكنك التعامل مع الهاتف على أنه غير وهمي، وقم فيه بتركيب مكافح فيروسات، وجدار ناري، وفي بي أن وحامي شاشة خاص به.

الأمر جيد، كلما قمت بتركيب طبقات حماية أكثر فهذا أفضل. بالطبع يعتمد على سرعة معالج اللابتوب ومواصفاته بالإضافة لسرعة شبكة الأنترنت عندك.

وبالطبع بت تدرك الآن أن تطبيق الهواتف الوهمي هو بحد ذاته طبقة حماية إضافية.

لا أريد التوصية بتطبيقات محددة، بل الأفضل أن يقوم جميع الإخوة بالبحث بأنفسهم، السبب أنهم خلال بحثهم سوف يقرأون أكثر، ويفهمون أكثر، ويتعلمون أكثر.

حسناً الآن تصور معي هذا المشهد ...

أنت تستخدم محاكي جوالات في اللابتوب، يوجد داخل الهاتف الوهمي في بي أن من شركة روسية، ومكافح فيروسات من شركة صينية، وجدار ناري وحامي شاشة.

ثم في اللابتوب نفسه تستخدم في بي أن من شركة كورية، مكافح فيروسات من شركة أخرى، جدار ناري وحامي شاشة ....

ثم أرسلت رسالة عبر تطبيق مشفر بالكامل End to End

مرحباً بك في عالم التعقيد ....

إن وقعت حزمة رسالتك هذه بيد جهة ما في العالم وكذب تطبيق التشفير وقام بفك تشفيرها، سوف يصطدم بتشفير شركة في بي أن الهاتف الوهمي، سيذهبون لها، ستفك التشفير، سوف تصطدم بتشفير شركة الفي بي أن في اللابتوب ... الخ

حسناً ماذا لو تم اختراق الهاتف الوهمي؟ سوف يصطدمون بحماية اللابتوب نفسه.

باقي الهواتف الوهمية في أمان تام.

وعليه فإننا ننصح في الهواتف الوهمية أن لا تقوم بجعل كل عملك في هاتف واحد فقط، قسمها، باختصار أجعل من سوف يوقع بك يذوق الأمرين قبل التمكن من هذا إن استطاع.

ولكن بطبيعة الحال فإن هناك نصيحة هامة لا تتجاهلها فيما يتعلق في الفي بي أن

نصحك بالإبتعاد عن التطبيقات المجانية

هذا الأمر غاية بالضرورة، خصوصاً في مكافح الفايروسات والجدار الناري والفي بي أن.

استخدموا التطبيقات الرسمية المباعة، واختاروا تطبيقات من شركات ودول مختلفة كما ورد شرحه سابقاً، وادفعوا ثمن الخدمة من خلال العملات المشفرة "البتكوين".

- ليس لدي لابتوب، لا يمكنني الحصول عليه الآن، هل يوجد بديل للمحاكيات مخصص للهواتف؟

نعم يوجد ولكن ليس بنفس القوة والكفاءة، سوف يتم شرحها.

- ماذا لو سقط جهازي بيد العدو؟

هنا تأتي مرحلة الإبتكار. حيث يمكنك ابتكار طرق حماية إضافية.

شخصياً لا أوصي أبداً أن تكون جميع ملفاتك على اللابتوب، بل يكون جهاز اللابتوب مجرد وسيلة فقط.

بينما تقوم بتركيب تطبيقات الهواتف الوهمية وكل ما يلزمك من تطبيقات أخرى على ذاكرة خارجية "فلاش مثلاً" بسعة عالية جداً 1 تيرا بايت مثلا أو 500 جيجا.

وبمجرد سحب هذا "الفلاش" من الجهاز فعندها يصبح فارغ بلا فائدة لأي جهة كانت.

والجميل في هذا الأمر أن بمقدورك أن تعود وتستخدم هذا "الفلاش" في أي جهاز آخر.

بالطبع الذاكرة الخارجية لابد أن تكون محمية بنظام تشفير، لذلك عند اختيارها اختر نوع الذاكرات الذي يكون محمي بكلمة مرور، او قم بتركيب نظام تشفير عليها.

في أسوأ الأحوال، إذا تعرضت للمداهمة، كل ما يلزم الأمر هو إخراج "الفلاش" في ثانية واحدة ثم تكسيرها أو رميها في مكان يصعب الوصول إليه.

- هل من إجراءات اضافية؟

بالطبع، الحماية عالم لا ينتهي، والابتكار هو مفتاح النجاح بها.

قد يأتي أخ الآن ويستنبط ويبتكر فكرة جديدة من الشرح أعلاه تقوي من بروتوكولات الحماية هذه.

مكافح الفايروسات والجدار الناري

الحقيقة الصادمة حول إختراق الأجهزة هي أنه لا توجد أي طريقة في العالم تمكنك من التأكد يقيناً أن جهازك غير مخترق، لهذا عليك الإفتراض دائماً أن الجهاز مخترق وتتخذ الإجراءات التي تمنع المخترق من الوصول إلى أي بيانات.

- مكافح فايروسات
- جدار ناري
- في بي أن تشفير
- مانع تصوير الشاشة
- المحاكيات
- طبقات الحماية داخل المحاكيات
- برمجيات التشفير العامة والخاصة
- استخدام المنصات الموثوقة والمشفره End to End

هذه كلها وسائل لحماية البيانات وحايتك من الإختراق حتى إن حدث سلفاً.

ولكن بشكل عام يمكنك أن تعرف بوجود اختراق إن وجدت عملية خروج للبيانات من جهازك غير مصرح بها.

غالباً هذه مهمة الجدار الناري الذي سوف ينهبك لها كذلك ومكافح الفيروسات بالطبع لذلك احرص دائماً على اختيار الأفضل.

حالياً فجميع برامج مكافحة الفايروسات الموثوقة والمدفوعة بالطبع تقدم لك خدمات كاملة لحمايتك من الإختراق مثل الجدار الناري، وتعمل على تحديث نفسها باستمرار وفحص جهازك بصورة دورية كذلك وفحص أي ملف جديد تقوم بتحميله في الجهاز.

لذلك لا تستهين ابداً بأهمية مكافح الفايروسات بل وبأهمية شراء نسخة مدفوعة كاملة منه وعدم الإعتماد على النسخة المجانية فقط.

فمكافح الفايروسات يعتبر طبقة حماية إضافية هامة للغاية، لا تستخدم الإنترنت بدونه.

في 1% من الحالات لن يتمكن الانتي فايروس من اكتشاف البرمجيات الضارة، وهنا نحن نتكلم عن برمجيات تم برمجتها من قبل فرق مختصة على الأغلب هي فرق حكومية تمكنت من التحايل على الانتي فايروس.

لذلك فإن اتباعك لسبل الحماية التي تم شرحها في هذه الدروس سوف يحميك بإذن الله تعالى حتى من ال 1% المتبقية.

الدراسة التالية تقدم لك أفضل أنواع الأنتي فايروس التي يمكنها استخدامها

https://cybernews.com/best-antivirus-software/antivirus-for-windows-11

أو يمكنك البحث بنفسك عن مواصفات البرامج والخدمات التي تقدمها.



يعمل مكافح الفيروسات والجدار الناري على كشف أي برمجيات خبيثه وحماية جهازك من الإختراق

الأرقام الوهمية

- سمعت كثيراً بمصطلح الأرقام الوهمية فما هو الفرق بينها وبين الأرقام الحقيقية؟

يعتقد الكثير من الناس أن أهمية الأرقام الوهمية تنحصر في الحصول على رقم بدون اسم حقيقي وبدون الحاجة لإبراز وثيقة إثبات الشخصية، إلا أن أهميته تتجاوز هذا القدر بكثير.

عندما تقوم بوضع شريحة هاتف SIM Card في هاتفك الجوال فإن أول ما تفعله هذه الشريحة هو الحصول على رقم IMEI الخاص بجهازك، وهذا هو رقم فريد لا يتكرر لجهازين في العالم ابداً، إن وقع بيد أجهزة المخابرات الدولية فعندها عليك حرق الجوال والتخلص منه فوراً، لأنه لن ينفعك بعدها التخفي ابداً.

ليس فقط شريحة الهاتف هي من يمكنها الحصول على رقم IMEI بل حتى جميع تطبيقات الجوال التي تقوم بتحميلها من المتجر أو غير المتجر، مثل تطبيق التلجرام أو واتس أب أو غيرها من التطبيقات.

فإذا مثلاً قمت بوضع شريحة جوال داخل الهاتف، فعلت بها تطبيق التلجرام ثم قمت بالتخلص من الشريحة، هنا قد تظن أنك في أمان من أي خطر يتعلق بالشريحة! وهذا غير صحيح، فقد تم رصد رقم IMEI الجهاز الخاص بك ومعرفة أن مستخدم هذا الجهاز هو من استخدم الشريحة الفلانية يوماً ما، عندها إن قمت بعمل حساب تلجرام جديد من شريحة مختلفة فلن ينفعك هذا التخفي شيء، لأن رقم IMEI هو نفسه لا يختلف.

تقاطع المعلومات وكسرات الخبر التي تتركها خلفك بلا مبالاة خطر حقيقي فلا تتجاهله

على سبيل المثال يتواجد في منطقة إدلب السورية شركة هواتف رسمية، تقدم لك شريحة جوال بسعر 1 دولار فقط، يمكنك تفعيل كل أنواع البرامج عليها، وكذلك يمكنك الحصول على شريحة جديدة في أي وقت إن فقدت شريحتك الأصلية.

في الوقت الذي قد يصل به سعر الرقم الوهمي الواحد إلى دولار أو نصف دولار لتفعيل برنامج لمرة واحدة فقط، فإن هذه الشركة تقدم لك خدمة كاملة برقم رسمي وإنترنت وكل الميزات الكاملة بسعر فقط 1 دولار أمريكي!

حسناً فكر، 1 دولار فقط فما هو مكسب الشركة؟

نعم بالضبط، المكسب هو معلومات وبيانات، كما ذكرنا سابقاً حول تطبيقات الفي بي أن المجانية، الهدف دائما هو أنت، فأنت السلعة.

لذلك فإننا ننصح دوماً باستخدام الأرقام الوهمية، وذلك لأنك باستخدامها فإنك لا تحصل فقط على رقم بدون اسم ولكنك سوف تحصل على ميزات الآمان التالية جميعها.

- عدم ارتباط الرقم بشخصيتك الحقيقة
- عدم وجود شريحة وبالتالي استحالة معرفة IMEI الجهاز من خلاله أو التجسس عليه
- الأرقام الوهمية تنتقل بين الناس سريعاً، فإن امتلكت رقم اليوم ثم تركته فعلى الأغلب سوف يستخدمه شخص أخر بعد وقت قريب للغاية وهكذا كان قبل استخدامك له، لذلك فسوف تجد على الرقم الواحد عشرات ومئات حسابات التطبيق نفسه التي تم ويتم تفعيلها باستمرار، بينما الشريحة تدخل مرحلة حذف قد تصل إلى 6 أشهر أو سنة كاملة قبل حصول شخص غيرك على نفس الرقم بعد تركك له.
- سهولة ومرونة تبديلها وامتلاكها فيمكنك الحصول على عشرات ومئات الأرقام الوهمية دون تعقيد ودون الحاجة لمغادرة كرسيك أو تبديل شرائح.
- سوق الأرقام الوهمية هو سوق لا مركزي، فلا يوجد جهة في العالم يمكنها السيطرة عليه.
- يمكنك شراء هذه الأرقام باستخدام العملات الرقمية المشفرة.
- يمكنك اختيار أي دولة في العالم فلا يمكن حصرك ضمن نطاق جغرافي محدد.
- بعض أنواع هذه الأرقام تسمح لك باستقبال الرسائل المتعددة بل وحجز الرقم لفترة زمنية واستقبال المكالمات الصوتية عبر النت.

- كيف تعمل الأرقام الوهمية؟ هل تديرها أجهزة مخابرات؟

للإجابة على هذا السؤال لا بد أن نفهم آلية عمل هذه الأرقام، فهي تشبه إلى حد كبير عمل الإنترنت نفسه اليوم وحتى عمل العملة الرقمية المشفرة مثل البتكوين وباقي العملات اللامركزية .

إن سوق الأرقام الوهمية هو سوق لا مركزي ينشط في الإنترنت المظلم (الديب ويب) يديره أشخاص مختلفين لأغراض تجارية، ولا نتحدث عن أشخاص معدودين بل جميع الناس يمكنهم بيع الأرقام الوهمية في الديب ويب، ويوجد عشرات الآلاف من الأشخاص حول العالم يفعلون هذا بالفعل.

حيث يمكن لأي شخص أن يقوم بشراء أجهزة ومعدات خاصة تسمح له بتركيب ألف شريحة جوال مثلاً وربطها مع موزع أرقام وهمية في الديب ويب والحصول على مبلغ مالي مقابل كل رسالة تفعيل تصل لأحد هذه الأرقام.

فرقمك الوهمي الذي قمت لتوك بتفعيل تطبيق التلجرام عليه قد يكون مالكه هو شاب في جنوب أفريقيا لديه عشرات ومئات الأرقام الأخرى بعيداً عن بيته الآن ويتقاضى المال مقابل رسائل التفعيل بشكل آلي.

إن هذا السوق اللامركزي يؤمن لك الحماية الإضافية، فلا يمكن لأي جهة بالعالم أن تسيطر عليه بالكامل ولا حتى على أجزاء منه، إنه يشبه كثيراً السوق اللامركزي للعملات الرقمية المشفرة.

- كيف يمكن الحصول على كميات كبيرة من الأرقام الوهمية بسعر أرخص؟

إن كنت مستخدم عادي تشتري الأرقام الوهمية عبر تطبيقات ومواقع الأرقام فغالباً فإنك سوف تصطدم بسعرها المرتفع! الذي قد يصل في بعض الأحيان وبعض الدول إلى أكثر من دولار، ويتراوح بين 20 سنت و 5 دولار بل و 10 دولار احياناً لرسالة التفعيل الواحدة!

فماذا لو كنت تود تفعيل 10 أرقام يومياً؟

عملنا في الجهاد الإعلامي يحتاج الكثير والكثير من هذه الأرقام!

لايمكننا تحميل هذه الميزانية العالية بالتأكيد!

لذلك عندها عليك تجاوز هذه البرامج والتطبيقات والتعامل بشكل مباشر مع مزودين هذه الخدمات عبر الديب ويب والحصول على الأسعار التنافسية، والذين لايمكن التعامل معهم إلا برمجياً فعندها عليك أن تمتلك برمجياتك الخاصة التي تخولك الدخول إلى هذا العالم المظلم نفسه.

أو استخدام النوع الثاني من الأرقام وهي الأرقام الوهمية الغير مشروعة إن صح التعبير، حيث تعمل فرق مختصة في الإنترنت المظلم على التحايل من خلال إنشاء أرقام تبدو حقيقة بالكامل وبيعها بأسعار أرخص، هذه الأرقام غير مضمونة دائما فقد تواجه رسالة من التطبيق يقول لك هذا الرقم غير حقيقي أو هذا الرقم لا يصلح! لكنها تستحق التجربة والمحاولة نظراً لسعرها التنافسي.

أخيراً، هذا السوق لا مركزي في كل شيء بما فيه الأسعار وينطبق عليه مبدأ العرض والطلب.

فكلما زاد الطلب على رسائل تفعيل تطبيق معين سوف يزيد سعر هذه الرسائل، وكلما قل الطلب سوف يقل السعر.

لذلك فإننا ننصح المجتمع الجهادي الإلكتروني بتبديل التطبيقات باستمرار والبحث عن أكثرها أماناً وهذا ماسوف يتم شرحه في باب تطبيقات التواصل المشفرة.

تطبيقات الجوال والمواقع الإلكترونية

بالتأكيد سمعت عن الفرق الشاسع في الأمان بين استخدام موقع إلكتروني وتطبيق للجوال او حتى برنامج للكمبيوتر!

قد تطرقنا في فصل سابق إلى خطر رقم IMEI الجهاز، وكما يمكن لأي تطبيق يتم تحميله إلى هاتفك الجوال الحصول على هذا الرقم فإن بامكانه فعل الكثير مثل فتح باب خلفي لإختراقك من خلاله والتجسس على بياناتك ومعلوماتك.

لذلك فإننا ننصح الجميع بتجنب تحميل وتركيب تطبيقات الجوال الغير موثوقة عالمياً والغير موصى بها من قبل فرق الحماية والأمن الرقمي العالمي المختلفة.

ولكن ماذا عن الموقع الإلكتروني؟ هل ينطبق عليه هذه القواعد؟

بالتأكيد لا، فلا يمكن للموقع الإلكتروني الذي تستخدمه عبر المتصفح أن يحصل على أي من هذه البيانات الخاصة بك، كما لايمكن إختراق الجهاز من خلاله مالم تقم طواعية بتحميل برمجيات من هذا الموقع.

ولكن لا بد من الإنتباه من تلك المواقع التي قد تطلب منك إضافة ملحقات إلى المتصفح لديك، حيث لن يكون بمقدورك استخدام الموقع إلا بعد الموافقة على رسالة إضافة ملحق خاص بالموقع إلى المتصفح extensions حيث ينطبق على هذه الملحقات البرمجية الخاصة جميع ما ينطبق على التطبيقات من مخاطر أمنية، قم دوماً بفحص الملحقات في متصفحك extensions chrome والتأكد من خلوها من أي ملحقات لمواقع إلكترونية لا تعلم عنها ولم تصرح بها، كذلك استخدم متصفحات الإنترنت الآمنة مثل متصفح Brave.

واحرص دوماً على إجراء بحث واسع حول أي تطبيق أو متصفح تستخدمه خصوصاً تلك المتصفحات التي تقدم لك خدمات البروكسي والتخفي، تحقق من تبعيتها وحقيقة مشغليها.

- كيف اعرف أن الموقع الإلكتروني آمن للتصفح؟

بما أن الموقع الإلكتروني الذي تستخدمة لا يطلب منك تحميل أي ملفات إلى جهازك أو أي ملحقات للمتصفح فهو آمن تماماً على جهازك من الإختراق.

ولكن ما زال هناك بعض المعلومات التي يمكن للموقع الحصول عليها، مثل نوع المتصفح أو عنوان الآي بي الخاص بك.

ولتجنب هذا عليك دوماً الحرص على استخدام وسائل الحماية التي تم شرحها في هذه الدروس.

فالمتصفح آمن تماماً من هذه الناحية، أي أنه لا يمكن للمتصفح أن يخترق هاتفك، مستحيل وقطعياً . ولكن يمكنه مثلا معرفة معلومات معينة مثل الآي بي الخاص بك ، نوع المتصفح الذي تستخدمه، وبعض الأمور التي لا تهدد أمنك بشكل مباشر ، وهذا ليس بالضرورة أي أن هذا يعتمد على الموقع الإلكتروني نفسه فيمكن لمدير هذا الموقع رفض استقبال عنوان الآي بي الخاص بك.

في بعض المواقع يتم استخدام الخدمات السحابية، أشهرها هو

https://www.cloudflare.com

فعندما تطلب عنوان الموقع يتم أولاً تحويلك الى موقع الكلاود هذا ثم من خلاله تخرج البيانات مشفره وتعود إليك مشفره، هو بمثابة البروكسي أو الفي بي أن للمواقع.

ومن ميزاته كذلك أنه يخفي هويتك أنت أي هوية الآي بي الخاص بك (إن قام مالك الموقع بتفعيل هذا النوع من الحماية) فيرسلك إلى الموقع الإلكتروني بآي بي خاص بموقع الكلاود وبهوية مزيفه من الكلاود فلا يمكن لمدير الموقع نفسه معرفة تفاصيل كثيرة عنك قد يتمكن من معرفتها إن دخلت الموقع بشكل مباشرة بدون هذا الوسيط وهو الكلاود.

كيف تعرف ان الموقع يستخدم هذه الخدمة؟

ادخل هنا

https://whois.is

اكتب عنوان الموقع الإلكتروني الذي تود البحث عنه في مربع البحث مثلا google.com

سوف يعطيك معلومات تفصيلية عن هذا النطاق ، من مالكه ورقم هاتفه .. الخ

طبعا في المواقع الرسمية تكون معلومات حقيقة بينما في المواقع الجهادية مثلا كلها تكون مزوره غير حقيقة وغالباً لن تظهر لك حيث أن كثير من المواقع تطلب إخفاء هذه المعلومات.

ولكن بعض المعلومات لايمكن إخفائها ويهمنا منها هو هذا Name Server

إن أشار النيم سيرفر هذا إلى موقع CLOUDFLARE.COM أو موقع مشابه له فهذا يعني أنك قبل دخول الموقع فانك تدخل موقع CLOUDFLARE والذي بدوره سوف يقوم بتشفير إتصالك بطبقة حماية جديدة، ثم إرسالك للموقع النهائي.

يوجد استخدامات كثيرة للكلاود وفي الحقيقة فإن مدراء المواقع قد لايهم الكثير منهم حماية زوارهم، ولكن يهمهم حماية الموقع نفسه، فالكلاود يحمي الموقع من الزوار كذلك ، يحميه من الإختراق والهجمات ... الخ، هو طبقة حماية اضافية للموقع مثل الفي بي أن ، حيث أن المواقع الإلكترونية خصوصاً في الديب ويب تستخدم طبقات حماية مشابهة تماماً لطبقات الحماية الشخصية التي تم شرحها في هذه الدروس.

بالعودة إلى السؤال المهم: هل يمكن اختراق الجهاز عبر موقع الكتروني من المتصفح.

الجواب : لا

لأن الموقع الإلكتروني لا يدخل إلى نظام التشغيل الخاص بك، فبما أنك لم تقم بتحميل شيء من الموقع واكتفى تواجدك به على التصفح فقط فهذا يعني أنه من المستحيل اختراق جهازك من خلاله.

ولكن عليك الإنتباه جيداً إلى اضافات المتصفح Extensions كما ورد ذكره.

بعض المواقع عند دخولها سوف يظهر لك في الأعلى في الزاوية تقول لك نود تركيب إضافة إلى المتصفح لتتمكن من استخدام هذا الموقع اسمها بالانجليزي Extensions، لا تفعل ذلك مالم تكن واثق من الموقع تماماً.

لان هذه الإضافة تعتبر مثل التطبيق، انت من خلالها سوف تعطي هذا المواقع صلاحيات واسعة في جهازك. ونعم يمكن اختراقك من خلالها.

وبالحديث عن اختراق الأجهزة من خلال الروابط لا بد لنا من الحديث عن بيجاسوس الإسرائيلي..

سمعنا أنه بمجرد إرسالهم رابط الكتروني للضحية او الإتصال معه عبر اي تطبيق لمدة 10 ثواني فقط فإنه يتم اختراقه !!

إذاً الموقع الإلكتروني يمكنه اختراق الجهاز صحيح؟

برنامج بيجاسوس لا يخترق الجهاز عبر المتصفح بل يستخدم ثغرات موجوده سلفاً في نظام التشغيل .أحدث ضجة عالمية كبيرة، وضحيته الأكبر كانت شركات مثل جووجل وأبل، حيث أنه اخترق أنظمة تشغيلها نفسها ووجد ثغرات بها.

فهو لا يعمل على زراعة شيء داخل جهازك من خلال إختراق الجهاز نفسه يفتح له باب خلفي تقليدي كما شرحنا في مشاركات سابقة، بل يستخدم ثغرات وابواب خلفية موجوده في نظام التشغيل نفسه سلفاً، عيوب في نظام التشغيل اكتشفها فريق عمل بيجاسوس .

والرابط الإلكتروني أو المكالمة الهاتفية التي تصلك هذه من أجل تهيئة عملية استغلال هذه الثغرة. بالمحصلة هو لا يفتح باب خلفي بل يستخدم باب خلفي موجود في النظام نفسه أو يزرع برمجية خبيثة تفتح له باب خلفي خاص من خلال باب خلفي موجود بالنظام سلفاً أو في التطبيق.

مثلا في حالة تطبيق بجاسوس الذي ورد ذكره سابقاً، تمكن فريق العمل من اكتشاف ثغرة في الواتس آب قاموا من خلال إجراء اتصال مع الهدف وحتى إذا لم يجيب الهدف فإنهم من خلال هذا الإتصال قاموا بتمرير برمجيات خبيثة، لأنه بات هناك نوع من تبادل البيانات بين المرسل والمستقبل وهو ما نتج عنه حالة الرنين ، إذاً يوجد تبادل بيانات ووجدوا الثغرة منها.

لذلك عليك الإنتباه بشكل عام في الوسط الجهادي من هؤلاء الذين لا تعرفهم جيداً ويتصلون عليك بسبب وبدون سبب، مثل ان يقوم معرف تجهله بعمل اتصال معك !! سوف تلغي أنت الإتصال ولن تقبله ولكن إن كان هذا الإتصال هدفه تمرير برمجية خبيثة إلى جهازك فقد مررها وانتهى الأمر.

أفهم وطبق دروس الأمن السيبراني التي تم تقديمها في هذه الدروس وسوف تكون كافية لحمايتك بإذن الله تعالى حتى من بيجاسوس.

المخاطر لا تندرج فقط على جهازك الخاص بل قد يأتيك الخطر من جهاز آخر لم تكن تتوقع أن يتم إختراقك من خلاله! وهنا لابد لنا الحديث عن أجهزة التلفاز الذكية والإرتباط مع شبكة الإنترنت من خلال هاتف أخر أو خدمة البلوتوث.

التلفاز الحديث يرتبط بالإنترنت وبالتالي يوجد إتصال بينه وبين النت ويمكن اختراقه، تنطبق عليه جميع ماتم ذكره على الهاتف من مخاطر، ولكن من هذا المهتم في معرفة برامجك التي تتابعها!! والأهم أنه غير منتشر.

ولكن الخطورة تكمن حينما تقوم بربط الهاتف الذكي مع جهاز الجوال الخاص بك. عندها من الممكن نقل هذه البرمجيات الى الجوال من خلال التلفاز.

لذلك ستكون كارثة كبيرة لو أنك مثلاً سجلت بريداً إلكتروني في التلفاز نفس الذي تستخدمه في جوالك، أو وضعت فيه تطبيق أو سجلت دخول في أي تطبيق قد يشير الى شخصيتك الجهادية.

والأفضل عدم إجراء هذا الربط مع التلفاز إن كان الأخ مستهدف على نطاق واسع.

البلوتوث قطعاً يمكن اختراقك منه وتمرير برمجيات خبيثة لا تحتاج لشرح كبير بعد ماتم شرحه حول التلفاز. أنت تعطي البلوتوث صلاحية تبادل بيانات مع هاتفك، اصبح راوتر ولكن خطير جدا حيث أن صاحب جهاز البلوتوث يمكنه مباشرة تمرير البرمجيات الخبيثة إلى هاتفك.

بشكل عام بمجرد إعطاء صلاحية لأي جهاز لتبادل البيانات مع جهازك فإنك تعرض نفسك لخطر الإختراق إن كان ذلك الجهاز يحتوي برمجيات خبيثة لديها القدرة على الإنتقال تلقائياً.

تطبيقات التواصل المشفرة

نحن بحاجة لتطبيقات التواصل لما تقدمه من مرونة وسرعة في الإداء، ولكن هذا الميزات لها ثمن باهض وقد يكون معلوماتك وأمنك وحياتك هي الثمن !

لذلك عليك تحري الدقة والمصداقية قبل استخدام أي تطبيق تواصل عبر الإنترنت.

حسب الدراسة التالية التي تم تقديمها من موقع nordvpn

https://nordvpn.com/blog/most-secure-messaging-app

لاحظ أن هذه الدراسة القيمة اهتمت ولخصت التطبيقات حسب جوانب رئيسية مثلاً

- E2E encryption التشفير ايند تو ايند
- Self-destructing messages التدمير الذاتي للرسائل
- Collects data about users and their contacts جمع المعلومات عن المستخدمين والاحتفاظ بها
- Tracks users' social media activity تتبع نشاطات المستخدمين عبر وسائل التواصل الإجتماعي
- وميزات أخرى سوف تجدها مكتوبة تحت التطبيق

علامة الزائد الخضراء تعني توصية

علامة السالب الحمراء تعني عيب

من أهم نقاط الضعف الأمنية في أي تطبيق هو تتبعه للنشاطات أو جمع البيانات، هذا يتم لغايات تجارية في كثير من الأحيان ولكنها بالطبع تعني التجسس عليك مهما حاولوا تجميل المصطلحات والتسميات.

لاحظ مثلاً تطبيق مثل سيجنال العيب الوحيد الذي تم اسناده له هو حاجته لرقم هاتف، فمثلاً استخدام رقم هاتف وهمي يجعله بلا عيوب حتى الآن.

كما أن التلجرام جيد خصوصاً في المحادثات المشفرة بالكامل، ولكن مشكلته أنه التلجرام، الخصوصية فيه لم تعد مضمونة ابداً حيث بات هدفاً لجميع الجهات المختصة بالحرب على الإرهاب.

فضلاً عن وجود تطبيقات اقوى منه بالتشفير والخصوصية أعلى وحسب الدراسة هي

Threema

Wickr

Signal

ومع هذا عندما تستخدم هذه التطبيقات وفي الأمور الغاية في الأهمية يجب عليك ان تقوم بتشفير رسائل بها عبر برمجيات تشفير الرسائل، وهذه تعتبر طبقة حماية إضافية تستخدم عادة في المراسلات الهامة.

مفهوم التشفير وبرامج التشفير الخاصة

التشفير هو عبارة عن ممارسة حماية المعلومات باستخدام الخوارزميات المشفرة.

يمكن أن تكون المعلومات غير نشطة (مثل ملف على القرص الصلب)، أو متنقلة (مثل الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر)، أو قيد الإستخدام (أثناء الحوسبة على البيانات).

والتشفير أنواع يمكن مثلا فك الشيفرة بعشر سنوات وممكن شيفرة أخرى فكها بمائة عام.

باختصار: كل شيفرة يمكن فكها.

هذا طبيعي لأنها بالأصل مصنعه من اجل فكها على جهاز المستقبل وإلا ما الفائدة منها إن كان يستحيل فكها؟

ولكن كل شيفرة لها مفتاح خاص لايتم فكها إلا به حتى لو لم تكن تعلم عن هذا المفتاح أنت، ولكنه موجود ويكون في خلفية التطبيق.

يمكنك ملاحظة هذا مثلا في حسابك التلجرام

إذا كنت تستخدم حساب التلجرام على جهازين فسوف تلاحظ ان جميع محادثاتك على الجهاز الأول تظهر بالكامل على الجهاز الثاني كذلك.

ولكن هذا لا يحدث في حالة الغرفة المشفرة !

لماذا؟ لأن تشفير الغرفة أي مفاتيح فك تشفيرها يكون مرتبط بجهازك الذي استقبلت او قمت بعمل الغرفة المشفرة منه، ونقصد المحادثة المشفرة، بالتالي لايمكن فك شيفرة الرسائل على الجهاز الثاني نظراً لعدم توفر مفتاح فك التشفير، بالطبع حسب تعهد التلجرام فإن هذا النوع من المحادثات المشفرة هي من نوع تشفير End to End.

ورغم هذا كله يمكن فك الشيفرة، مهما بلغت قوتها.

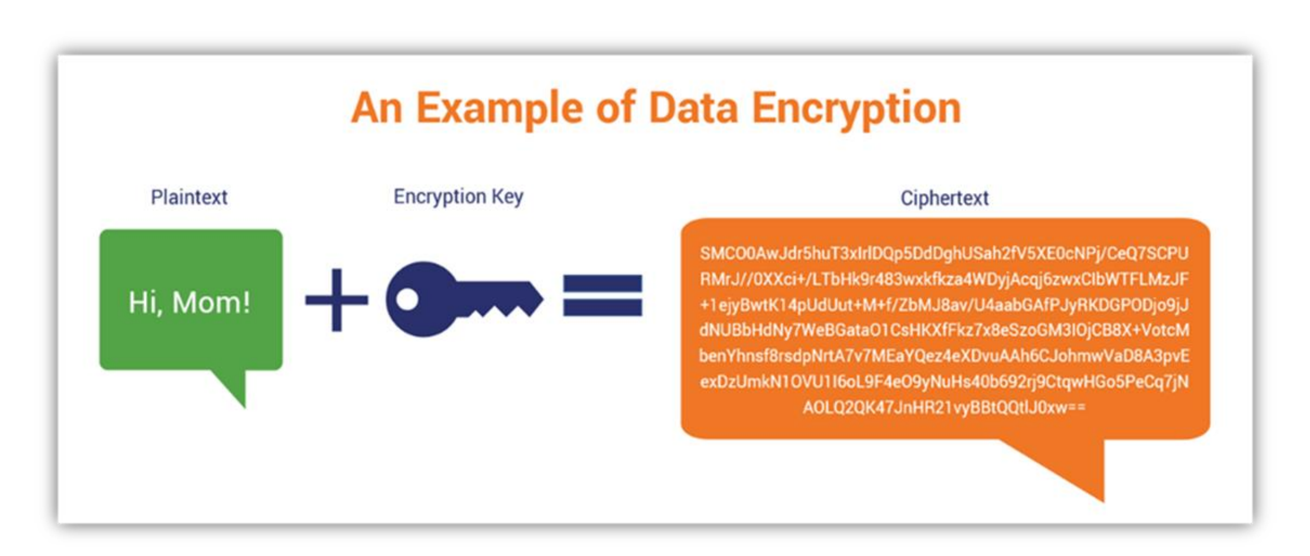
فالمسألة فقط مسألة وقت وذلك من خلال التجريب العشوائي أو مبدأ القوة الغاشمة، حيث يتم وضع النص المشفر في كمبيوتر بمواصفات جبارة، وعندها يبدأ الكمبيوتر بتجربة جميع الأرقام والرموز والأحرف الموجودة في لوحة المفاتيح بشكل عشوائي حتى يصل إلى مفتاح فك التشفير الصحيح.

مثلا لنفرض ان مفتاح فك التشفير كان هكذا 123، في هذه الحالة فإن أي جهاز حساب لن يستغرق أكثر من ثواني حتى يحصل عليه وينجح بفك الشيفرة، لأنه سهل جدا.

ولكن اذا كان هكذا sadsada@^&@@#^#^&%#& ##&#^*#^*&#^IG#JH

سوف ينجح بالنهاية بفك التشفير ولكن ممكن بعد 100 عام أو 500 عام وربما أكثر، حسب قدرات جهاز الحساب.

فما بالك أن مفاتيح فك التشفير يكون مكون من عشرات الرموز والأرقام والأحرف! نظرياً يمكن فك الشيفرة وعملياً من المستحيل ذلك.



الرسالة + مفتاح التشفير = نص مشفر يستحيل فكه إلا من خلال مفتاح التشفير نفسه

أنواع التشفير مختلفة ودرجات قوتها متباينة، بل ويمكنك عمل تشفير مركب مثلا نفرض النص التالي "مرحباً يا أخي"، تقوم بتشفيره على نظام تشفير معين، ثم تقوم بتشفير التشفير نفسه على نظام آخر ، وهكذا.

ولكن بشكل عام لا داعي لهذا إن كان التشفير قوي للغاية لأن أعظم الكمبيوترات على وجه الأرض "المعروفة" سوف يلزمها عمل مئات السنيين من أجل فك تشفير كلمة واحدة إن تم تشفيرها بأنظمة تشفير قوية.

نستخدم التشفير الخاص في حالات التراسلات المهمة مثل نقل ملف أو نص هام للغاية، فبعد اتباع جميع الإجراءات الأمنية التي تم تقديمها في هذه الدروس نقوم كذلك بتشفير المادة عبر برمجيات تشفير خاصة، ومفاتيح خاصة لفك التشفير لا يعرفها إلا الطرف الآخر.

مثال بسيط على عملية التشفير باستخدم مفتاح فك تشفير عبارة عن كلمة مرور عبر الموقع

https://www.gillmeister-software.com/online-tools/text/encrypt-decrypt-text.aspx

- اكتب النص الذي تريده، اكتب في مكان كلمة المرور أي كلمة مرور تريدها ثم اختر Encrypt.
- قم بعمل التشفير سوف يظهر لك النص المشفر في الأسفل.
- انسخ هذا النص وارسله الى صديقك والذي يعرف كلمة المرور سلفاً.
- سوف يقوم بأدخال النص وكلمة المرور ويختار Decrypt.
- وسوف يتم فك الشيفره في الأسفل.

يمكنك تشفير النص أولاً بكلمة مرور، ثم تشفير الشيفرة بكلمة مرور ثانيه

ثم صديقك عليه ان يفكها أولاً بكلمة المرور الثانية ليحصل على الشيفرة الأولى، ثم يفك الشيفرة الأولى بكلمة المرور الأولى، هذه شيفرة مركبه.

بالبحث في جووجل يمكنك ايجاد تطبيقات تشفير عالمية مشهورة ومضمونه، سوف تجدون الكثير من هذه البرامج الموثوقه لذلك فلن نوصي بأي تطبيق أو برنامج محدد، كما أن البرامج تتيح لك إمكانية تشفير مجلد بأكلمة بكل مافيه من ملفات.

حذف الملفات نهائياً مع منع استعادتها

سؤال يسأله الكثيرون، كيف يمكنني حذف الملفات من الجهاز بشكل نهائي دون إمكانية استعادتها أبداً، أو حتى كيف يمكنني التحقق من أن البرمجة الضارة التي تم إختراق الجهاز من خلالها لن تعيد تشغيل نفسها مرة أخرى بعد عمل فورمات للجهاز كاملاً؟

هل يمكن لبعض البرمجيات الخبيثة المتطورة أن تبقى مختبئة في مكان داخل الهاردسك بكامل بنيتها ثم تعيد تشغيل نفسها بعد الفورمات؟

هل يمكن استعادت الملفات بعد عمل فورمات أو بعد حذفها نهائياً من الجهاز؟

الجواب للسؤالين هو: نعم

لذلك فنحن ننصح الأخ بصورة دائمة إن لم يكن لديه خبرة كافيه بحماية نفسه أن يقوم بتغيير الجوال في حال أي شكوك حول عملية إختراق.

ولكن بإذن الله تعالى في هذ الفصل سوف نتعلم سوياً كيف نحمي أنفسنا ونتعامل مع الإختراق عبر البرمجيات، وكيف نمحي أي أثر لها ونمنعها من تشغيل نفسها بعد الفورمات، وكذلك منع استعادت الملفات المحذوفة.

البرمجيات ومنها برمجيات الإختراق كلها ترتبط مع نظام التشغيل للهاتف او بمعنى أخر هي تدخل الى القرص الصلب (الهاردسك) للجهاز.

فإذا قمت بتبديل الهاردسك او تنظيفه تماماً لن يعود لها أي أثر مالم يكون لديها قدرة على إعادة تشغيل نفسها، وبعض انواع البرمجيات الخبيثة المتطورة لديها القدرة على ذلك، حيث يمكنها إعادة تشغيل نفسها تلقائياً إن بقيت داخل الهاردسك ببنيتها الكاملة.

ما هو الهاردسك؟

هو وحدة تخزين البيانات، يتم التحكم به بواسطة وحدة التحكم في الجهاز فهي من تقول له ماذا يفعل.

بالتأكيد سمعت من قبل عن أن اللغة الأصلية للحاسبات هي 0 و 1 وهذه تعني فتح إغلاق، حالة ال 0 تعني مغلق وحالة ال 1 تعني مفتوح. ولا أود الخوض معكم بهذه التفاصيل الميكانيكية حول الجهاز ولكن الهاردسك تكون البيانات كلها مخزنة به على شكل أصفار وأحاد، 0 و 1. مثلا شيء كهذا 01011110011100101 لا يفهم الجهاز ولا يمكن تخزين اي شيء داخل الهاردسك إلا 0 أو 1، في الحقيقة هو لا يخزن 0 و 1 اصلاً بل يفعل شيء اخر ولكن يمكن اختزال الأمر بهذه الطريقة.

عندما تبدأ استخدام الجهاز يكون الهاردسك فارغ تماماً أو شبه فارغ ومع استخدامك له يبدأ يمتلىء بالمعلومات، ويبدأ بالكتابة على أجزاء الهاردسك ولن يعود للكتابة على الجزء الذي كتب عليه أولاً إلا بعد إنتهاء تعبئة الهاردسك كله.

هذا يعني انك عندما تقوم الأن بتحميل صورة ثم تحذفها فإنه لا يتم مسحها من الهاردسك ومازال من الممكن استعادتها بكل سهولة وهذا لأن قابلية المسح غير موجود في الهاردسك أصلاً، إنما هو يخفيها فقط ويحرر المساحة الخاصة بها للسماح بالكتابة فوقها أي وضع مادة أخرى، مما يتهيء لك أنه قد حذفها، وفي الحقيقة هو يضعها تحت بند مسموح الكتابة فوقها ثم يخفيها.

وعندما ينتهي الجهاز من استخدام الهاردسك كله سوف يعود للبداية ويبحث عن الاجزاء التي تم اخفاء ملفاتها ويكتب فوقها من جديد، وهكذا.

فمن الممكن أن تكون حذفت صورة قبل 10 سنوات ولكن حتى هذه اللحظة لم يملتىء الهاردسك الخاص بك ومازال حذفها من نوع حذف رقم 0 أي لم يتم كتابة اي شيء فوقها.

وهذا يعني أنه يمكن استعادتها بسهولة حتى إن مر عليها 10 سنوات.





في الشركات يتم تدمير الهاردسك المنتهي استخدامه وكذلك الأجهزه بهذه الطريقة، لتجنب أي مخاطر محتملة من استعادت البيانات

لهذا فنحن ننصح في حالة رغبتك بتنظيف الهاردسك ان تستخدم تطبيقات وظيفتها الكتابة على جميع أجزاء الهاردسك الغير مستخدمه، بما في ذلك التي تم استخدامها سابقاً وحذفت بياناتها.

هذه التطبيقات سوف تعمل على الكتابة مرة ومرتين وثلاثة وصولاً إلى 10 مرات وأكثر فوق الهاردسك وفقط الاجزاء الغير مستخدمة حالياً.

مما يعني استحالة استعادت البيانات المحذوفه، بما فيها البرمجيات الضارة والخبيثة مثل الفايروسات أو برمجيات التجسس، حيث سوف تعمل على اعطابها تماماً وبالتالي عدم قدرتها على تشغيل نفسها بعد فرمتت الجهاز إن كانت هذه البرمجيات تمتلك هذه القدرة.

فضلاً عن هذا فإنها سوف تعمل على تقسيم أجزاء الملفات نفسها واتلافها تماماً وتوزيعها داخل الهاردسك مما يعني استحالة أن تتمكن البرمجيات الخبيثة إن وجدت من تجميع نفسها من جديد، وبنفس الطريقة استحالة أن تتمكن أي جهة من استعادت الملفات المحذوفة بعد حذفها.

من أشهر هذه التطبيقات للجوال هو تطبيق Andro Shredder.

والذي عند تشغيله سوف يقوم بفحص جميع الأجزاء الغير مستخدمة من الهاردسك بما فيها تلك التي طلب حذف بياناتها وسوف يقوم بالكتابة فوقها مرة ومرتين وصولاً إلى 10 مرات، فضلاً عن هذا فإنه سوف يعمل على تقسيم وتفتيت هذه البيانات نفسها مما يعني استحالة تجميعها من جديد مرة أخرى من قبل المختصين أو تجميعها هي لنفسها.

لكن عليك أن تعلم أن استخدام التطبيق بكثرة سوف يقصر من عمر الهاردسك الخاص بك، لا مشكلة في هذا مقابل ما يوفره لك من أمان.

كما أن أغلب برامج الأنتي فايروس تقدم خدمة تقسيم وحذف الملفات نهائياً وتنظيف الهاردسك بالكامل تجدها تحت خيارات Shredder.

ومن أشهر برامج الأنتي فايروس التي تقدم هذه الخدمة هو برنامج bitdefender.

وهذا المصطلح File Shredder يعني حذف مع تدمير الملف في الهاردسك أي تقطيع الملف، فما يفعله بالضبط هو انه لايحذف الملف فقط بل يقطع بنيته الأصلية ويوزعها على الهاردسك ، فلا يمكن للملف أن يجمع نفسه من جديد أو أن يجد أحد أجزاءه ويجمعها سويا، فهذا بات أصعب من البحث عن إبرة في أكوام من القش وليس كومة قش واحدة.

مثلا هذا الشرح لعملية الحذف، ولكن هذا الحذف يكون لملف واحد فقط، وفي بعض أنواع الأنتي فايروس تجد هذه الميزة موجودة لكامل الهاردسك.

https://www.bitdefender.com/consumer/support/answer/2179/



تعمل برامج تدمير البيانات على تقطيعها مما يجعل من المستحيل استعادتها من جديد

وهنا لا بد من التذكير بأمر هام للغاية

عندما نقول الهاردسك فنحن لا نقصد القسم C منه والذي جرت العادة بتحميل نظام التشغيل مثل الويندوز عليه.

فإن هذه الأقسام C , D , E , F مجرد أقسام وهمية لترتيب ملفاتك، فعندما نقول الهاردسك نعني كل أقسامه، الهارد بالكامل.

- ماذا أفعل بالملفات الموجودة أصلاً على الجهاز في حالة الشك بوجود إختراق؟

اولاً عليك نقل ملفاتك المهمة والاحتفاظ بنسخة منها، بعد نقلها من الجهاز المشكوك في إختراقه إلى وحدة تخزين خارجية (فلاش) وبعد أن تكون قد طبقت جميع أساسيات الحماية وقمت بتحميل انتي فايروس موثوق ومدفوع، فعند وضع الفلاش في الجهاز سوف يطلب منك فحص الفلاش كاملة، اترك الأنتي فايروس يقوم بفحص كل ملفاتها.

ثم لا تقوم بفتح إلا الضروري منها فقط، أي لا تعيد كل الملفات إلى الهاردسك فقط ما تحتاجه منها إن لزم الأمر.

في 99% من الحالات سوف يتمكن الأنتي فايروس من اكتشاف البرمجيات الضارة وتنظيفها أو حذف الملفات نهائيا إذا فشل في تنظيفها مع الحفاظ على سلامة بنية الملف الأصلي.

لذلك من الأفضل قبل أن تقوم بفحصها أن يكون لديك نسخة ثانية منها على فلاش ثاني. هذا يحدث مثلاً أن يكون لديك ملف مهم، لكن اكتشف الأنتي فايروس برمجية ضاره ولم يتمكن من تنظيف الملف فسوف يقوم بحذفه نهائياً وتقطيعه.

عندها سوف تفقد الملف كله.

إن حدث أمر مثل هذا قم بتشغيل الفلاش على جهاز ثاني لا تستخدمه وانسخ النص الذي تريده إن كان مهم لهذه الدرجة.

في 1% من الحالات لن يتمكن الأنتي فايروس من اكتشاف البرمجيات الضارة، وهنا نحن نتكلم عن برمجيات تم برمجتها من قبل فرق مختصة على الأغلب هي فرق حكومية تمكنت من التحايل على الأنتي فايروس.

عندها لاقدر الله إن حدث هذا فسوف يحمي اتصالك وبياناتك باقي اجراءات الأمان المتبعة.

والشيء بالشيء يذكر...

لايمكننا التحدث عن خطورة الملفات مالم نعرج على ما يسمى بال Meta Data

الميتا داتا هي معلومات تكون موجود في أي ملف وأنت لا تعرف بوجودها.

فمثلاً إذا قمت بالتقاط صورة من جهازك وأنت قد منحت الكميرا صلاحيات الموقع الجغرافي، فإن إحداثياتك الجغرافية في لحظة التقاط الصورة سوف يتم تخزينها داخل ملف الصورة دون أن تعلم بذلك.

كذلك سوف يتم تخزين معلومات كثيرة مثل اسم الجهاز وقت التقاط الصورة ومعلومات أخرى قد تبدو لك ليست ذات اهمية ولكنها بالتاكيد مهمه جداً لأنها تعطي معلومات تفصيلية عن جهازك نفسه وعن الصورة لا تعلم عنها.

هذه المعلومات اسمها ميتا داتا أو بيانات الميتا وتكون موجود داخل الملف لايمكنك إظهارها ولكن يمكن إظهار جزء منها من خلال عرض تفاصيل إضافية عن الصورة بعد فتحها بالجهاز.

المعلومات الأكثر والأخطر يمكن رؤيتها من خلال تطبيقات خاصة بقراءة معلومات الميتا.

- هل هذا يعني أن كل صورة أصورها وأرسلها على التيليجرام تحتوي هذه المعلومات؟

حسناً في حالة التيليجرام ، الواتس آب، فإن هذه التطبيقات تقوم تلقائياً بإعادة هيكلة الميتا، أي حذف الميتا الأصلية وتغييرها وذلك مع تغيير دقة الصورة نفسها مثلاً. ولكن ليس كل شيء.

بينما إذا قمت بارسال ملف أو صورة عبر موقع تحميل أو عبر البريد الإلكتروني أو بأي طريقة أخرى فإن معلومات الميتا يمكن استخراجها وبالتالي معرفة كثير من الأشياء التي كنت تجهل وجودها.

- كيف يمكنك تغيير هذه المعلومات؟

ابحث في جووجل عن هذا

metadata changer

سوف يظهر لك تطبيقات وبرامج وأيضاً مواقع إلكترونية تمكنك من رفع الملف ثم تغيير معلومات الميتا ثم تحميله من جديد.

الخاتمة

إن أصبنا فإنه من فضل الله علينا وإن اخطأنا فمن الشيطان.

عالم الحماية واسع للغاية والتقنيات تتبدل باستمرار، وما هو آمن اليوم قد لا يكون هكذا غداً. لذلك فإننا ننصح دوماً بمواكبة هذا العلم وتحديث قناعات المجتمع الجهادي باستمرار حول سبل الحماية المتبعة.

تم إعداد هذا الكتاب بالتعاون مع مجلس التعاون الإعلامي الإسلامي IMCC

في حال وجود أي إستفسار أو سؤال لا تتردد بالتواصل مع إخوانك في المجلس عبر طرق التواصل المتاحة أو عبر المؤسسات المنتسبة للمجلس.

وآخر دعوانا أن الحمد لله رب العالمين

القسم التقني – الحرب الإلكترونية

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)